

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA & KAHOOT EDU, INC.,
Petitioner

v.

AVIEL D. RUBIN,
Patent Owner

Inter Partes Review Case No. IPR2023-00693
Patent No. 9,064,376

**PETITIONERS' OPPOSITION TO PATENT OWNER'S
MOTION TO AMEND U.S. PATENT NO. 9,064,376**

Mail Stop Patent Board
Patent Trial and Appeal Board
P.O. Box 1450
Alexandria, VA 22313-1450

February 23, 2024

LIST OF EXHIBITS

1001	Rubin, U.S. Patent 9,064,376 (“the ’376 Patent”)
1002	Declaration of Sigurd Meldal, Dr.Scient.
1003	Prosecution History File Wrapper of the ’376 Patent (excerpts)
1004	U.S. Patent 9,497,565 (“Zha”)
1005	CN 2013/10674692 (“Zha-Priority-Application”)
1006	Certified English translation of the <i>Zha-Priority-Application</i>
1007	U.S. Patent Pub. 2015/0011318 (“Takahashi”)
1008	PCT/JP2012/007595 (“Takahashi-Priority-Application”)
1009	Certified English translation of <i>Takahashi-Priority-Application</i>
1010	U.S. Patent Pub. 2014/0006485 (“Tsushima”)
1011	U.S. Patent 9,591,083 (“Gumbula”)
1012	U.S. Patent Pub. 2012/0017236 (“Stafford”)
1013	U.S. Patent 9,330,531 (“Wakeford”)
1014	Patent Owner’s Preliminary Infringement Contentions in <i>Rubin v. Kahoot! ASA et al.</i> , Civil Action No. 6:22-cv-00236 (W.D. Tex.) (Sept. 28, 2022)
1015	U.S. Patent Pub. 2012/0253841 (“’841 Application”)
1016	U.S. Patent Pub. 2012/0209770 (“’770 Application”)
1017	U.S. Patent Pub. 2014/0121015 (“Massing”)
1018	U.S. Patent Pub. 2006/0058088 (“Crawford”)
1019	March 10, 2023 Email from W.Beard (Petitioner to E.Benisek (PO)
1020	March 14, 2023 Email from E.Benisek (PO) to D.Adams (Petitioner)
1021	FedEx Proof of Delivery of Service Copy of Petition
1022	Declaration in Support of Motion for <i>Pro Hac Vice</i> Admission (Brian C. Banner)
1023	U.S. Patent Pub. No. 2012/0240203 (“Kling”)

1024	L. St. Clair <i>et al.</i> , “Password Exhaustion: Predicting the End of Password Usefulness,” ICISS 2006, LNCS 4332, pp. 37-55 (Springer-Verlag Berlin Hiedelberg 2006)
1025	U.S. Patent No. 7,865,950 (“ <i>Lipetz</i> ”)
1026	Deposition Transcript of Patent Owner’s expert Dr. Patrick Traynor – February 15, 2024 (condensed)
1027	Second Declaration of Sigurd Meldal, Dr. Scient
1028	P. Traynor <i>et al.</i> , “From Mobile Phones to Responsible Devices,” Security Comm. Networks 2011, 4:719–726, (Wiley Online Library, August 28, 2010)

TABLE OF CONTENTS

I.	INTRODUCTORY STATEMENT	1
II.	PATENT OWNER FAILS TO MEET STATUTORY AND REGULATORY REQUIREMENTS FOR AN MTA.....	2
A.	Patent Owner Does not Show Written Description Support.....	2
B.	“Application Specific Authentication Information” (cls. 26, 41).....	2
C.	“Providing a Notification by the Application on the Second Device that the Connectivity has been Disrupted” (cl. 30).....	6
III.	THE AMENDED CLAIMS ARE INDEFINITE	7
A.	“Application Specific Authentication Information”.....	7
B.	“Providing a Notification by the Application on the Second Device”	8
IV.	PO’S CONSTRUCTION OF “SENSITIVE INFORMATION” IS CONTRARY TO THE SPECIFICATION’S EMBODIMENTS	9
V.	GROUND 9: CLAIMS 26–29, 31, 34, AND 40–41 ARE OBVIOUS OVER <i>KLING</i> AND A POSITA’S KNOWLEDGE	11
A.	Overview: <i>Kling</i>	11
B.	Obviousness in View of <i>Kling</i> and a POSITA’s Knowledge	12
VI.	PETITION GROUNDS 1–6 (“ <i>ZHA</i> GROUNDS”).....	16
A.	Response to PO’s Arguments RE: <i>Zha</i> Grounds.....	18
VII.	<i>ZHA</i> GROUNDS COMBINED WITH <i>KLING</i>	20
VIII.	PETITION GROUNDS 7–8 (“ <i>TAKAHASHI</i> GROUNDS”)	20
A.	Response to PO’s Arguments RE: <i>Takahashi</i> Grounds	23
IX.	<i>TAKAHASHI</i> GROUNDS COMBINED WITH <i>KLING</i>	24
X.	MOTIVATION TO COMBINE // ANALOGOUS ART.....	24

TABLE OF AUTHORITIES

CASES

<i>Ariad Pharms., Inc. v. Eli Lilly & Co.</i> , 598 F.3d 1336 (Fed. Cir. 2010) (en banc).....	2
<i>Danxiao Info. Tech. Ltd. v. Shenzhen Svakom Tech. Co.</i> , PGR2022-00050, Paper 36 (Jan. 19, 2024)	6
<i>Ex Parte Talkowski</i> , Appeal No. 2012-002290 (PTAB May 24, 2013).....	24
<i>Intel Corp. v. FG SRC LLC</i> , IPR2020-01449, Paper 53 (PTAB Mar. 1, 2022).....	2
<i>Intel Corp. v. Qualcomm Inc.</i> , No. 2020-2092, 2022 WL 880681 (Fed. Cir. Mar. 24, 2022).....	25
<i>Interactive Gift Exp., Inc. v. Compuserp Inc.</i> , 256 F.3d 1323 (Fed. Cir. 2001) (en banc).....	9
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	25
<i>Lectrosonics v. Zaxcom</i> , IPR2018-01129, Paper 33 (PTAB Feb. 25, 2019)	2
<i>Liebel–Flarsheim v. Medrad, Inc.</i> , 358 F.3d 898 (Fed. Cir. 2004)	9, 10
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	7
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005) (en banc).....	9
<i>Uniloc 2017 LLC v. Hulu, LLC</i> , 966 F.3d 1295 (Fed. Cir. 2020)	11

I. INTRODUCTORY STATEMENT

The Board should find (1) PO's Non-Contingent Motion to Amend ("MTA") does not satisfy PO's burden to show a reasonable likelihood that PO has satisfied the statutory and regulatory requirements for an MTA; and (2) Petitioner has shown a reasonable likelihood that claims 26–41 are unpatentable.

First, PO fails to show written description support for its substitute claims. PO leaves it up to the Board to guess how cited passages allegedly support the claims. This failure is fatal, particularly where there is no written description support for (1) newly minted term "application specific authentication information" (cls. 26, 41) and (2) new phrase "providing a notification by the application on the second device..." (cl. 30). Second, PO's amendments render the claims indefinite. PO does not offer a construction of "application specific authentication information," and PO's arguments about what is *not* "application specific authentication information," render the meaning of the term even more unclear. Further, "the application on the second device" (cl. 30) is indefinite because it lacks antecedent basis or, alternatively, because it is ambiguous and subject to multiple interpretations.

Claims 26–41 are unpatentable in view of the Grounds raised in the Petition and/or new Grounds that include additional prior art. PO's argument for patentability relies on (1) an incorrect construction of the term "sensitive information" that is contrary to disclosed embodiments, (2) a misreading of the claims to require the

recited information to be “generated by the application” “at the server,” (3) a legally incorrect view of what can qualify as analogous art, and (4) an incorrect analysis of a POSITA’s motivation to combine references.

II. PATENT OWNER FAILS TO MEET STATUTORY AND REGULATORY REQUIREMENTS FOR AN MTA

A. Patent Owner Does not Show Written Description Support

PO did not meet its burden to “set forth written description support ... for each proposed substitute claim.” *Lectrosonics v. Zaxcom*, IPR2018-01129, Paper 33 at 7 (PTAB Feb. 25, 2019). Rather than explain how any specification passages support PO’s amended claims, PO simply provided a table of string cites. MTA at 4–7. It is well-established that providing string cites without explanation does not meet a PO’s burden to establish written description support. *See, e.g., Intel Corp. v. FG SRC LLC*, IPR2020-01449, Paper 53 at 89 (PTAB Mar. 1, 2022) (citing *numerous* Board decisions holding that a list of string citations without explanation does not satisfy PO’s burden to show written description support).

B. “Application Specific Authentication Information” (cls. 26, 41)

The test for written description “is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). “Application

specific authentication information,” is not found in the original ’376 Patent application (Ex-2005), and PO has not offered a claim construction for the term.

Petitioner (and the Board) are left to guess (1) what the term means and (2) whether a POSITA would understand the patentee to have possession of “application specific authentication information” when the application was filed. Forcing Petitioner (and the Board) to engage in this guesswork in the first instance is highly prejudicial, especially where PO ignores specification passages that appear pertinent to the meaning of this term (*see* Ex-2005 ¶72 (discussing “application specific” components)), and where, at the same time, PO argues a narrow meaning in order to distinguish the Petition’s prior art. PO should not be allowed to coin a new claim term and avoid discussing its meaning so that it can distinguish prior art in this forum while leaving the door open to other constructions in district court.

PO identifies Fig. 10 and ¶¶26, 33, 75, 83, 89, 90, and 92 of the ’995 App (Ex-2005) as providing written description support. MTA at 4 (element [26c]), 7 (element [41d]). None do. Ex-1027 ¶¶8–27 (Meldal Decl.).

¶26: This discusses authentication information for an application running on an individual’s second device—not “at the sever.” Ex-1027 ¶11. In contrast, the amendments to claims 26 and 41 relate to “application specific authentication information” for “the same application at the server.” Ex-1027 ¶¶7, 11.

¶33: This is unrelated to authentication information. Ex-1027 ¶13.

¶75 / Fig. 10: These disclose two passwords authenticated by the server. Ex-1027 ¶15. However, PO's expert argues that authentication by *a server* is **not** "application specific." Specifically, PO's expert (Dr. Traynor) distinguished authentication by *Tsushima's* server as not disclosing "application specific authentication information" because authentication information *for the server* (i.e., where the server performs the authentication) is allegedly not authentication information specific to *the application*. Ex-1026, 106:8–108:8. Fig. 10 and ¶75 disclose authentication by "[t]he central server" and not an application. Ex-1027 ¶15. Under Dr. Traynor's rationale, ¶75 and Fig. 10 do not support "application specific authentication information." *Id.* Additionally, PO and its expert argue that "device specific" authentication information is not "application specific" authentication information. MTA at 17; Ex-2004 ¶9. Fig. 10 shows that one password is assigned to the "first device" and the second password is assigned to the "second device." Because each password is tied to a specific device and is, therefore, "device specific" under PO's reasoning, ¶75 and Fig. 10 provide support for "device specific," but not "application specific authentication information." Ex-1027 ¶¶16–17.

¶83: In view of PO's exclusion of "device specific" information (MTA at 17; Ex-2004 ¶9), ¶83 does not provide support for "application specific authentication information" because the security keys and cryptographic tokens are specific to the second device. Ex-1027 ¶19. "[I]f an authentication token is used on the second

device, then the user will be limited to using that specific device whenever using the application with the central server.” Ex-2005 ¶92. Thus, under PO’s own reasoning, the “device specific” security keys and cryptographic tokens in ¶83 do not provide support for “application specific authentication information.” Ex-1027 ¶19.

¶89: This describes a “device specific” random number that is used for registration of the second device “at registration time.” Ex-1027 ¶¶21–23. PO’s reasoning that “device specific” authentication information cannot be “application specific authentication information” forecloses the use of this “device specific” random number as providing support for the new claim term. Ex-1027 ¶21. Additionally, the random number is for registering the second device whereas the “application specific authentication information” is for authentication. Ex-1027 ¶22.

¶90: This repeats the disclosure found in (i) Figure 10 and ¶75, and (ii) ¶83; and does not provide support for the same reasons. Ex-1027 ¶25.

¶92: The disclosed authentication token is “device specific,” which does not support the new claim term as discussed above with respect to ¶83. Ex-1027 ¶27. Further, the passage discusses authentication by a separate application running on the second device. *Id.* In contrast, “application specific authentication information” in the claims is for “the same application at the server.” *Id.*

The cited passages together: PO cites to examples that, even taken together, do not inform a POSITA of the abstraction in the substitute claims. This is especially

true considering PO's arguments that create confusion as to the scope of "application specific authentication information," i.e., arguing without explanation that "device specific" authentication information is outside the scope of "application specific authentication information." This manufactured distinction is not found in the specification, a fact further confirming "application specific authentication information" is an abstraction with no written description support. *See Danxiao Info. Tech. Ltd. v. Shenzhen Svakom Tech. Co.*, PGR2022-00050, Paper 36 at 24 (Jan. 19, 2024) (no written description support where "the specification gives an example and would support a claim to that example, but it does not inform skilled artisans of the abstraction Patent Owner seeks to claim ...").

C. "Providing a Notification by the Application on the Second Device that the Connectivity has been Disrupted" (cl. 30)

Claim 30 recites "providing a notification by the application on the second device that the connectivity has been disrupted." First, "the application on the second device" lacks antecedent basis. Ex-1027 ¶30. Claim 26 (from which 30 depends) recites an "application at the server." *Id.* A person of ordinary skill in the art would not understand this limitation as providing antecedent basis for the new amendment "the application on the second device." *Id.*

PO cites to ¶33 and original claim 5 of the '995 App as alleged support. MTA at 5. ¶33 discloses the server switching communication mechanisms in the case of a network disruption but does not disclose providing a notification. Ex-1027 ¶32.

Moreover, this passage does not mention an “application on the second device”—it discusses the functionality of “the server.” *Id.* Further, the server terminating the session does not disclose any particular action (or lack thereof) on the part of the application on the second device, much less the specific action of notifying the second device that connectivity has been disrupted. *Id.* Original claim 5 also does not provide written description support for this new phrase. Ex-1027 ¶34. While claim 5 discloses providing a notification on the second device, it does not disclose doing so “by the application on the second device,” as claimed. Ex-1027 ¶¶34–35.

III. THE AMENDED CLAIMS ARE INDEFINITE

“[A] patent is invalid for indefiniteness if its claims, read in light of the specification ... and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014).

A. “Application Specific Authentication Information”

The term “application specific authentication information” (cls. 26, 41) is indefinite under 35 U.S.C. § 112(a). This is a new term that is not found in the patent, and PO does not offer a claim construction. Instead, PO argues that “device specific” information cannot be “application specific.” This apparent (narrow) construction of the term is not based on a plain meaning and finds no support in the specification. Ex-1027 ¶40. In fact, the patent is to the contrary, as it discloses using device specific

information (a device specific password) for authentication (Fig. 10). The issue is further confused by Dr. Traynor's admission that "device specific" information may be used as part of "application specific authentication information." Ex-1026 at 127:20–128:14, 130:17–131:19. Dr. Traynor also suggested that whether "device specific" information could be "application specific" depends on whether the information was provided by a manufacturer as opposed to a user or the system or something else. Ex-1026 at 125:14–123:16. Further, Dr. Traynor admits that passwords, which are "user specific," are also "application specific." Ex-1026 at 72:4–9, 132:18–22. There is no reason why "device specific" information cannot also be "application specific" when "user specific" information can be. Finally, PO's understanding of "application specific" appears to be contrary to passages in the specification (*see* Ex-2005 ¶72 (discussing "application specific" components)). Because PO provides no meaningful contours to the new term and uses it in contradictory ways, the term fails to inform a POSITA of its scope. Ex-1027 ¶40.

B. "Providing a Notification by the Application on the Second Device"

The phrase "providing a notification by the application on the second device" in claim 30 is indefinite under 35 U.S.C. § 112(a). First, "the application on the second device" lacks antecedent basis, rendering it indefinite. Second, the term is ambiguous because it is unclear whether the "the application" is on the server or on the second device. The added phrase "by the application" could refer to either "the

application on the second device” (i.e., as written) or “the application” at the server. Which application provides the notification is important to understanding the claim. Neither the specification nor the file history clarify this ambiguity. Consequently, the claim limitation fails to inform a POSITA of its scope. Ex-1027 ¶41.

IV. PO’S CONSTRUCTION OF “SENSITIVE INFORMATION” IS CONTRARY TO THE SPECIFICATION’S EMBODIMENTS

PO’s construction of “sensitive information” should be rejected because it improperly imports limitations from the specification, is contrary to the specification’s embodiments, and is contradicted by PO’s expert.

Under *Phillips*, claim terms “are generally given their ordinary and customary meaning.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). “If the claim language is clear on its face, then our consideration of the rest of the intrinsic evidence is restricted to determining if a deviation from the clear language of the claims is specified.” *Interactive Gift Exp., Inc. v. Compuserp Inc.*, 256 F.3d 1323, 1331 (Fed. Cir. 2001) (en banc). PO and its expert skip the first step in claim construction by failing to consider the ordinary meaning of “sensitive information.” Instead, they start their analysis by importing limitations from the specification. This approach is legally improper. See *Liebel–Flarsheim v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004) (“improper to read limitations from a preferred embodiment described in the specification . . . into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited”).

Importing limitations from the specification is especially problematic where it contradicts specification embodiments and renders other claim limitations non-sensical. PO proposes information is “sensitive” if it “is not automatically shared with the first device.” MTA at 10. However, the specification discloses an embodiment where sensitive information (e.g., hole cards) is shared automatically with the first device when the second device is not present. Ex-2004 ¶44 (citing Ex-1001 at 4:10–12). At step 718 of Figure 7, the system automatically “Send[s] hole cards to player’s first device.” Ex-1001-9; Ex-1027 ¶165. PO’s construction also renders claim 29 non-sensical. That claim recites information that “is *more sensitive* than the information received at the first device.” Ex-1027 ¶47. PO’s construction deems information sensitive or not sensitive, a binary classification, whereas claim 29 requires degrees of sensitivity (“more sensitive”). Ex-1027 ¶48. For the foregoing reasons, there is no “clear indication in the intrinsic record that the patentee intended the claims to be so limited.” *Liebel–Flarsheim*, 358 F.3d at 913.

Further, PO’s construction does not help determine what *is* and what *is not* “sensitive information.” Instead, it deems information “sensitive” based on what is done with the information (i.e., whether it is “automatically shared”)—not based on the information itself. In contrast, Dr. Traynor insisted that a social security number is sensitive regardless what is done with it (e.g., even if shared automatically with a first device) (Ex-1026 at 38:18–39:19), and similarly insisted that the super bowl

score is not sensitive regardless what is done with it (e.g., if not automatically shared with a first device, it is still not sensitive) (Ex-1026 at 44:12–49:17).

Dr. Traynor’s defense of PO’s construction conflicts with his use of the term “sensitive information” in his own articles (Ex-1028 at 720; Ex-1026 at 33:16–22) and his own admission that in the context of mobile banking (e.g., disclosed in the ’376 Patent), credit card and social security numbers are “sensitive information” regardless of what is done with them (Ex-1026 at 34:8–21). Outside of this IPR, Dr. Traynor uses “sensitive information” according to a plain meaning, i.e., defined by the contents of the information, not by what a system does with the information.

V. GROUND 9: CLAIMS 26–29, 31, 34, AND 40–41 ARE OBVIOUS OVER *KLING* AND A POSITA’S KNOWLEDGE

A. Overview: *Kling*

U.S. Patent Pub. No. 2012/0240203 (“*Kling*”) (Ex-1023) is prior art under 35 U.S.C. § 102(a) because it published September 20, 2012, prior to the ’376 Patent’s July 28, 2014 filing date. Ex-1023, [22][43]. *Kling* is listed on the face of the ’376 Patent but was not cited by the Examiner during examination. Ex-1001, [56] (References Cited). Consideration of *Kling* is appropriate because “substitute claims in an IPR proceeding have not undergone a patentability review by the USPTO, *see* 35 U.S.C. § 316, and so the ‘substantial new questions of patentability’ that ‘have not previously been considered by the [US]PTO’ include all patentability questions.” *Uniloc 2017 LLC v. Hulu, LLC*, 966 F.3d 1295, 1305–06 (Fed. Cir. 2020).

Kling is directed to enhancing online security for a user transacting with a server using a first device (e.g., a PC) by obtaining secondary confirmation from the user on a second device (e.g., a phone). Ex-1023, [57], ¶[0013]; Ex-1027 ¶¶66–78. In an online banking context, *Kling* discloses protecting against malware on the user’s first device (e.g., the PC). Ex-1023, Figs. 1–5, ¶¶[0013]–[0019]; Ex-1027 ¶¶68–78. In *Kling*, a user uses their PC to log into the banking application on the bank server and initiate a funds transfer. Ex-1023 ¶[0014]. For this, the banking application sends transaction web page information to the user’s PC. Ex-1027 ¶¶73–75. After receiving the transfer request, the banking application on the server seeks confirmation of the transfer by sending a secondary request to the user’s phone. *Id.* ¶[0017]. For this, the banking application sends transaction confirmation web page information to the user’s phone after the user logs into the banking application with a username and password. Ex-1027 ¶¶73, 76–77. After receiving confirmation from the user, the banking application on the server sends the result web page information for display on both the PC and the phone, and if the result on the PC is modified by malware, “the user will suspect foul play and cancel rather than confirm the transaction on the mobile device 515.” *Id.* ¶[0019]; Ex-1027 ¶¶73, 78.

B. Obviousness in View of *Kling* and a POSITA’s Knowledge

Claim 26: Obvious in view of *Kling* and a POSITA’s knowledge. Ex-1027 ¶¶73–78, 79–107. [26Preamble] is disclosed by bank server transmitting banking

information to a user's PC and a user's phone. [26a] is disclosed by web page information stored at bank server. [26b] is disclosed by banking application information ("first subset," includes transaction web page and results web page) being sent to the user's PC and transaction confirmation information ("second subset," includes transaction confirmation web page and results web page) being sent to the user's phone. [26c] is disclosed by the server requiring the user to login at both the PC and the phone using passwords (application specific authentication information), "ideally using a different password [on the phone] than on the PC." Ex-1023 ¶[0018]. [26d] is disclosed because (1) the first subset of information will not be sent to the PC without user login on the PC, (2) the second subset of information will not be sent to the phone without user login on the phone, and (3) the transaction confirmation web page (part of the second subset) is not transmitted to the PC, and the transaction web page (part of the first subset) is not transmitted to the phone. To the extent it is argued *Kling* does not disclose the "if and only if" requirement, it would have been obvious based on the POSITA's knowledge as evidenced by the "if and only if" disclosed in *Tsushima*. Ex-1027 ¶¶73–78, 79–107.

Claim 27: Obvious in view of *Kling* and a POSITA's knowledge. Ex-1027 ¶¶108–10. *Kling* discloses the same "results page 409" (results web page that is part of the first and second subsets) is sent to both the user's PC and the user's mobile phone. Ex-1027 ¶¶108–10.

Claim 28: Obvious in view of *Kling* and a POSITA's knowledge. Ex-1027 ¶¶111–12. *Kling*'s transaction web page displayed on the user's PC is non-sensitive (first subset), and the transaction confirmation web page (i.e., an invitation enabling approval of the transfer of funds and providing the means to do so (the "OK" response)) is sensitive (second subset). Ex-1027 ¶¶111–12.

Claim 29: Obvious in view of *Kling* and a POSITA's knowledge. Ex-1027 ¶¶113–14. *Kling*'s transaction web page displayed on the PC (received at the first device) is less sensitive, and transaction confirmation web page displayed on the phone (received at the second device, i.e., an invitation to approve or cancel the funds transfer via the "OK" response) is more sensitive. Ex-1027 ¶¶113–14.

Claim 31: Obvious in view of *Kling* and a POSITA's knowledge. Ex-1027 ¶¶115–18. *Kling* discloses transmitting the banking application's transaction web page (first subset) to the user's PC over the internet, which is a TCP/IP-based network. Ex-1023, Figure 1. *Kling* discloses transmitting the transaction confirmation web page (second subset) to the user's mobile phone over a cellular network. Ex-1023 ¶[0017]. A POSITA understands the TCP/IP-based network (internet) is an independent electronic communication network when compared to a cellular network. Ex-1027 ¶¶115–18.

Claim 34: Obvious in view of *Kling* and a POSITA's knowledge. Ex-1027 ¶¶119–23. *Kling* discloses sending web pages to displays on the user's PC (first

device) and mobile phone (second device). Ex-1023 ¶¶[0014]–[0018], Figure 4. These pages contain bank account information and transaction confirmation that are for exclusive viewing by the user. Ex-1027 ¶¶119–23.

Claim 40: Obvious in view of *Kling* and a POSITA’s knowledge. Ex-1027 ¶124. *Kling* discloses the first and second subsets are specific to the banking application and derive from functions within that application (e.g., a bank transaction function, e.g., to transfer money). Ex-1023 ¶¶[0014]–[0018], Fig. 4; Ex-1027 ¶124.

Claim 41: Obvious in view of *Kling* and a POSITA’s knowledge. Ex-1027 ¶¶125–39. [41Preamble] is disclosed by bank server transmitting information to a PC and mobile device. [41a] is disclosed by web page information stored at the bank server. If argued *Kling* does not disclose “storage,” that is obvious based on a POSITA’s knowledge that servers store information for applications running on them. [41a] is further disclosed by banking application information (“first subset,” includes transaction web page and results web page) and transaction confirmation information (“second subset,” includes transaction confirmation web page and results web page), which are specific to the banking application and generated by the banking application at the server. [41b] is disclosed by the banking server 107, which a POSITA understands would have a processor that is programmed. [41c] is disclosed by banking application identifying banking application information (first subset) to be sent to the user’s PC and transaction confirmation information (second

subset) to be sent to the user's mobile phone. [41d] through [41f] are disclosed as discussed for elements [26b] through [26d]. Ex-1027 ¶¶125–39.

VI. PETITION GROUNDS 1–6 (“*ZHA* GROUNDS”)

Claims 26–41 are obvious in view of the *Zha* Grounds and the POSITA's additional general knowledge that an application can require two different passwords for the same user accessing the application from different devices. Ex-1027 ¶¶140–62. Although the scope of new term “application specific authentication information” in claims 26 and 41 is unclear, PO cites to the use of two different passwords (e.g., Figure 10) as providing support. Ex-1027 ¶144. Based on this, it was well known by 2014 that password authentication could be used for a microblog like *Zha*, and that two different passwords could be used for different devices accessing the same account. Ex-1027 ¶¶144–49. The POSITA's knowledge is evidenced by *Kling*'s disclosure (discussed above), and by U.S. Patent No. 7,865,950 (“*Lipetz*”). Ex-1027 ¶¶144–49. *Lipetz* was filed in 2007, issued in 2011, and discloses that different passwords can be used in systems where information has varying degrees of sensitivity. Ex-1027 ¶¶147–49. *Kling* and *Lipetz* both relate to the field of computer security and to securing computer systems against malware. Ex-1027 ¶151. Thus, they both provide a motivation to combine a POSITA's knowledge of using different passwords with *Zha*'s microblog—i.e, to enhance security against malware in that system. *Id.*

Modifying *Zha* to require different passwords on the different devices would not be beyond the POSITA's skill and a POSITA would have a reasonable expectation of success in making this modification because, by 2014, implementing a password login authentication scheme was trivial. Ex-1027 ¶152. The triviality of the implementation is why *Zha* does not provide details regarding how it implements authentication. *Id.* This modification of *Zha* represents the simple substitution of one known element (single password associated with a single account) for another known element (multiple passwords associated with a single account) to obtain predictable results (enhanced security against malware). Ex-1027 ¶¶153–54.

Claims 26–29, 31–34, and 36–41: These claims are not modified from their corresponding original claims except for the “application specific authentication information” limitations added to independent claims 26 and 41. Thus, the *Zha* Grounds as modified above (POSITA's knowledge of multiple passwords) renders these claims obvious. Ex-1027 ¶155.

Claim 30: As discussed above, PO's addition of “by the application on the second device” renders this claim indefinite. Additionally, to the extent understood, it is obvious based on Petition Grounds 3–4 as modified by the POSITA's knowledge of multiple passwords (see above). Notably, PO did not dispute that *Gumbula* is properly combined with *Zha* in Grounds 3–4. PO's amendment of this claim to depend from original claim 3 (reciting sensitive and non-sensitive

information) does not require additional argument, as *Zha* discloses the sensitive and non-sensitive information (see Petition Grounds 1–2). Ex-1027 ¶¶156–58.

Claim 35: This claim depends from claim 30, which is indefinite. PO adds a limitation from original claim 10, which was addressed in Petition Grounds 5–6. Claim 35 is obvious based on Petition Grounds 5–6 as modified by the POSITA’s knowledge of multiple passwords (see above). Notably, PO did not dispute that *Stafford* is properly combined with *Zha* in Grounds 5–6 or that *Stafford* discloses the same limitation now recited in claim 35. A POSITA would be motivated to combine *Gumbula* with *Zha*’s private messaging interface as explained for Petition Grounds 3–4 (cl. 30), and would be motivated to combine *Stafford* with *Zha*’s game interface as explained for Petition Grounds 5–6 (cl. 35). Because *Gumbula* and *Stafford* modify different interfaces in *Zha*, a POSITA understands that they would not interfere with each other or otherwise impair the resulting system. Rather, a POSITA would reasonably expect success for this combination because it is the use of known techniques (heartbeat messages in *Gumbula* and graphical indicators/identifiers in *Stafford*) to improve similar devices (messaging interfaces and game interfaces) in the same way (providing notification of connection disruption for messaging and a visual link between two devices for gaming). Ex-1027 ¶¶159–62.

A. Response to PO’s Arguments RE: *Zha* Grounds

“Application Specific Authentication Information”: PO’s argument that *Zha*

does not mention “authentication information” (MTA at 13–14) ignores that Petitioner relies on obviousness, not anticipation. A POSITA would understand *Zha*’s disclosure of “logging in” could (and most likely would) be by means of entering a username and password. Ex-1027 ¶165. It is undisputed that password authentication for an application like *Zha*’s microblog (e.g., Facebook) is “application specific.” Ex-1027 ¶163; Ex-1026, 72:4–9 (“My username and password that I use for social media application, that’s specific to that application.”).

“Generated by the Application at the Server”: PO incorrectly argues that *Zha*’s private messages must be generated by the application at the server (MTA at 14). First, PO misreads the claims to require the “information” to be generated by the application, while that requirement relates only to the “subsets” of information. Ex-1027 ¶169. Second, PO’s interpretation is contrary to disclosed embodiments where, e.g., a user’s medical records are “sensitive” (Ex-2005 ¶77), and these records are created by doctors and are not “generated by the application” or “at the server.” Ex-1027 ¶170. Similarly, PO’s expert testified that a social security number would be “sensitive information (Ex-1026 at 41:18–42:4), but these are generated by the government, not by an application “at the server.” Ex-1027 ¶170.

Private Messages—Specific to the Application: PO suggests that *Zha*’s private messages are not “specific to the application” because direct messages are part of any “microblog such as Facebook or Twitter.” MTA at 14. This argument

should be rejected because it, too, is contrary to the disclosed embodiments. Ex-1027 ¶171. For example, users could play poker on any poker application, users could perform online banking tasks on any online banking application, etc. *Id.*

VII. ZHA GROUNDS COMBINED WITH KLING

If PO argues that a POSITA lacks knowledge of a user accessing an account using multiple passwords on multiple devices, it would be obvious to combine *Kling*'s use of multiple/different passwords with *Zha*'s microblog application. Ex-1027 ¶¶180–81. *Kling* provides the motivation to modify *Zha*'s system (to protect against malware), and a POSITA would have a reasonable expectation of success in making this modification because, by 2014, implementing a password login authentication scheme was trivial. Ex-1027 ¶¶180–81, 173–79, 152–54.

VIII. PETITION GROUNDS 7–8 (“TAKAHASHI GROUNDS”)

Claims 26–35 and 37–41 are obvious in view of the *Takahashi* Grounds alone because *Takahashi* discloses the use of “identification information” that is unique to each mobile terminal and used by the application to authenticate the same user logging in from different terminals. Ex-1027 ¶185. PO's assertion that the identification information is “device specific” and, therefore, not “application specific” (MTA at 17) is incorrect. *Takahashi*'s application stores the identification information and uses it in the current and in subsequent user accesses, thus confirming the information is “application specific” and different (unique) for each

of the user's terminals. Ex-1027 ¶¶185. PO does not provide any meaningful distinction between "device specific" information and "application specific" information, and PO's expert agrees that passwords are both "application specific" and "user specific." Ex-1026 at 72:4–9, 132:18–22. There is simply no reason why "device specific" information cannot also be "application specific," as in *Takahashi*.

Alternatively, obviousness lies in view of *Takahashi* and the POSITA's additional knowledge that an application can require two different passwords where the same user accesses it from different devices. Ex-1027 ¶¶186–206. *Takahashi* discloses a user using passwords to access the account with multiple devices. Ex-1027 ¶¶187–88. As in *Kling* and *Lipetz*, it was well known by 2014 that two different passwords could be used for different devices accessing the same account. Ex-1027 ¶¶189–93. *Kling* and *Lipetz* both provide a motivation to combine a POSITA's knowledge of using different passwords with *Takahashi*'s game system—i.e., to enhance security against malware in that system. Ex-1027 ¶¶194–96.

Modifying *Takahashi* to require different passwords on the different devices would not be beyond the POSITA's skill and a POSITA would have a reasonable expectation of success in making this modification because, by 2014, implementing a password login authentication scheme was trivial. Ex-1027 ¶196. This modification of *Takahashi* represents the simple substitution of one known element (single password associated with a single account) for another known element

(multiple passwords associated with a single account) to obtain predictable results (enhanced security against malware). Ex-1027 ¶197. Notably, PO’s expert agreed that *Takahashi* would read on the substitute claims if it required different passwords for the user’s different mobile terminals. Ex-1026 at 136:1–137:5.

Claims 26–29, 31–34, and 37–41: These claims are not modified from their corresponding original claims except for the “application specific authentication information” limitations added to independent claims 26 and 41. Thus, the Petition Grounds as modified above (POSITA’s knowledge of multiple passwords) renders these claims obvious. Ex-1027 ¶199.

Claim 30: PO’s addition of “by the application on the second device” renders this claim indefinite. Additionally, to the extent understood, it is obvious based on Petition Grounds 7–8 as modified by the POSITA’s knowledge of multiple passwords (see above). PO’s amendment of this claim to depend from original claim 3 (reciting sensitive and non-sensitive information) does not require additional argument, as *Takahashi* and the POSITA’s knowledge teaches the sensitive and non-sensitive information (see Petition Grounds 7–8). Ex-1027 ¶¶200–02.

Claim 35: This claim depends from claim 30, which is indefinite. Ex-1027 ¶¶203, 200. PO adds a limitation from original claim 10, addressed in Petition Grounds 7–8. *Id.* Claim 35 is obvious based on Petition Grounds 7–8 as modified by the POSITA’s knowledge of multiple passwords (see above). Ex-1027 ¶¶203–06.

PO does not dispute that *Takahashi* discloses “displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.” Ex-1027 ¶205 (citing Ex-1002 ¶¶269–76). Thus, *Takahashi* discloses the same limitation found in claim 35 for the same, undisputed reasons. Ex-1027 ¶¶203–06.

A. Response to PO’s Arguments RE: *Takahashi* Grounds

Login Process: PO misreads *Takahashi* in arguing that it does not disclose the claimed login limitations because its “login process ... is then followed separately by an authentication process.” MTA at 16–18. A POSITA understands the Figure 11 process of *Takahashi* would be well-known password login/authentication where *Takahashi*’s use of the word “login” represents the input and transmission of login credentials. After submission of those credentials, the server performs authentication similar to normal password authentication schemes. Ex-1027 ¶208.

“Sensitive Information”: PO’s argument that *Takahashi* does not disclose “sensitive information” (MTA at 18–19) should be rejected at least because it relies on PO’s incorrect claim construction of “sensitive information.” Even under PO’s incorrect construction, *Takahashi*’s user-specific information is “sensitive” because it is not automatically sent to the first terminal when two devices are used. Ex-1027 ¶¶210–12. Finally, PO did not dispute that “sensitive information” and “non-sensitive information” (claim 3, now substitute claim 28) or “more sensitive”

information (claim 4, now substitute claim 29) would have been obvious based on *Takahashi* and a POSITA's general knowledge of other games that could be played using *Takahashi*'s system. Pet. Grounds 7-8 (cls. 3-4). Those other games include poker, which includes hole cards that are "sensitive information." Ex-1027 ¶213.

IX. TAKAHASHI GROUNDS COMBINED WITH KLING

To the extent it is argued that a POSITA did not have general knowledge of a user accessing an account using multiple passwords on multiple devices, it would have been obvious to combine *Kling*'s disclosure of using multiple/different passwords with *Takahashi*'s game application. Ex-1027 ¶¶220-21. *Kling*'s malware protection motivates modification of *Takahashi* in this manner. Ex-1027 ¶221.

X. MOTIVATION TO COMBINE // ANALOGOUS ART

PO's arguments that Petitioner's prior art is not analogous (MTA at 19-23) and that there is no motivation to combine (MTA at 23-25) should be rejected because they are based on the legally incorrect premise that the prior art must address the same problem as the '376 Patent. This Board's Informative Decision in *Ex Parte Talkowski*, Appeal No. 2012-002290 (PTAB May 24, 2013), rejects PO's argument and confirms that the "§ 103 analysis focuses on what is claimed apart from the motivation of the inventor." *Id.* at 15. As explained in *Talkowski*, the Supreme Court rejected the same argument PO makes here, i.e., "unless the 'prior art references address[ed] the precise problem that the patent was trying to solve,' the problem

would not motivate an inventor to look to those references.” *Id.* at 16–17 (citing *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 419–20 (2007)).

Here, Petitioner’s § 103 analysis focuses on what is claimed, which is a system that requires authentication of a user at multiple devices using login credentials. The prior art in Petitioner’s grounds falls squarely within this field of endeavor. Ex-1027 ¶¶173–79, 214–19. In particular, *Zha*, *Tsushima*, and *Takahashi* all disclose the use of authentication for a user accessing an application from multiple devices. *Id.* Additionally, these references are within the field of online security since they each expressly disclose systems and methods for addressing user authentication in online computer systems similar to the system claimed in the substitute claims. *Id.*

Notably, PO does not attempt to address the Petition’s explanation why a POSITA would have been motivated to combine the prior art. Instead, PO merely points out differences between the references and argues in conclusory fashion that the references are “narrow in application.” *See* MTA at 23–25. PO does not cite any authority that prior art is not combinable if PO can point out differences in the references. If that were the rule, no combination would survive. Petitioner is “required to show only that there is something in the prior art as a whole to suggest the desirability of making the combination.” *Intel Corp. v. Qualcomm Inc.*, No. 2020-2092, 2022 WL 880681, at *4 (Fed. Cir. Mar. 24, 2022) (citations and quotations omitted). The Petition—and this Opposition—do that.

February 23, 2024
Date

/s/ R. William Beard, Jr.

R. William Beard, Jr. (Reg. No. 39,903)
Brian C. Banner (*Pro Hac Vice*)

Slayden Grubert Beard PLLC
401 Congress Avenue, Suite 1650
Austin, Texas 78701

Attorneys for Petitioners

CERTIFICATE OF SERVICE

The undersigned hereby certifies the above-captioned Petitioner's Opposition to Motion to Amend and exhibits were served in their entirety on February 23, 2024, upon the following parties by sending a copy via email to the following addresses:

Robert S. McArthur (mcarthur@vbllaw.com)

Eric W. Benisek (ebenisek@vbllaw.com)

Respectfully submitted,

/s/ R. William Beard, Jr.

R. William Beard, Jr. (Reg. No. 39,903)

Brian C. Banner (*Pro Hac Vice*)

SLAYDEN GRUBERT BEARD PLLC
401 Congress Avenue, Suite 1650
Austin, TX 78701
t: 512.402.3550
f: 512.402.6865

Attorneys for Petitioners