

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.

Case No. IPR2023-00693

Patent No. 9,064,376

**PATENT OWNER'S REPLY IN SUPPORT OF REVISED
NON-CONTINGENT MOTION TO AMEND
U.S. PATENT NO. 9,064,376**

June 14, 2024

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	CLAIMS 26, 28, AND 41 HAVE WRITTEN DESCRIPTION SUPPORT	1
III.	CLAIMS 32 AND 35 ARE NOT INDEFINITE	3
IV.	PATENT OWNER’S THEREBY CLAUSE IS LIMITING	4
V.	ZHA DOES NOT RENDER THE CLAIMS OBVIOUS.....	6
A.	<i>Zha</i> Fails to Disclose Several Key Limitations of Substitute Claim 26	6
B.	<i>Zha</i> Fails to Disclose Substitute Claim 28	11
C.	<i>Zha</i> Fails to Disclose Substitute Claims 27, 29, 31, 32, 34-36, 37, 39, 40 and 41	12
VI.	<i>KLING</i> DOES NOT RENDER THE CLAIMS OBVIOUS	12
A.	<i>Kling</i> Does Not Disclose the Limitations of Substitute Claim 26	12
B.	<i>Kling</i> Does Not Disclose Substitute Claim 28	15
C.	<i>Kling</i> Does Not Disclose Substitute Claims 27, 29, 31, 32, 34, 35, 39, 40, 41	15
VII.	TAKAHASHI DOES NOT RENDER THE CLAIMS OBVIOUS.....	16
A.	Takahashi Fails to Disclose Substitute Claim 26	16
B.	Takahashi Fails to Disclose the Limitations of Remainder of the Substitute Claims	18

VIII. <i>ZHA, TAKAHASHI</i> AND <i>TSUSHIMA</i> ARE NOT ANALOGOUS ART	18
--	----

TABLE OF AUTHORITIES

CASES

<i>Amarr Co. Requester & Cross-Appellant v. Wayne-Dalton Corp. Pat. Owner & Appellant</i> , No. 2011-005126, 2011 WL 2491036 (B.P.A.I. June 20, 2011)	5
<i>Hoffer v. Microsoft Corp.</i> , 405 F.3d 1326 (Fed. Cir. 2005).....	5
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014).....	3
<i>Novartis Pharms. Corp. v. Accord Healthcare, Inc.</i> , 38 F.4th 1013 (Fed. Cir. 2022)	1, 2

RULES

MPEP s 2173.05(E).....	3
------------------------	---

LIST OF EXHIBITS

Exhibit No.	Description
2001	FedEx Detailed Tracking Receipt dated 03/14/2023
2002	FedEx Detailed Tracking Receipt dated 03/15/2023
2003	Declaration in Support of Patent Owner's Motion for <i>Pro Hac Vice</i> Admission of Eric W. Benisek pursuant to 37 C.F.R. § 42.10(c)
2004	Declaration of Patrick Traynor, Ph.D. in support of Patent Owner's Non-Contingent Motion to Amend U.S. Patent No. 9,064,376
2005	U.S. Patent Application No. 14/444,995
2006	U.S. Provisional Application No. 62/008,561
2007	A Guide through 7 Microblogging Websites, published at https://www.linkedin.com/pulse/guide-through-7-microblogging-websites-realytviews/
2008	Third Declaration of Patrick Traynor, Ph.D. in support of Patent Owner's Reply
2009	Third Declaration of Patrick Traynor, Ph.D. in support of Patent Owner's Reply

I. INTRODUCTION

Patent Owner Dr. Aviel D. Rubin (“Rubin” or “Patent Owner”) submits this Reply to Petitioner’s Opposition to Patent Owner’s Revised Non-Contingent Motion to Amend (“Opposition” or “Opp.”) (Paper 27) certain claims of U.S. Patent No. 9,064,376 (“the ’376 Patent”).

II. CLAIMS 26, 28 AND 41 HAVE WRITTEN DESCRIPTION SUPPORT.

Petitioner challenges Substitute Claims 26, 28 and 41 as lacking written description support. Petitioner is incorrect.

Claim 26 and 41. Patent Owner further amended Substitute Claims 26 and 41 to require that the “application specific authentication information” used to log into the first and second device is “**not authentication information specific to a device.**” Petitioner argues that because the specification only discusses limiting the second device to authentication information not specific to a device, that similarly limiting the first device authentication lacks written description support.

To satisfy the written description requirement, a patent's specification must “reasonably convey[] to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” *Novartis Pharms. Corp. v. Accord Healthcare, Inc.*, 38 F. 4th 1013, 1016 (Fed. Cir. 2022). “For negative claim limitations . . . there is adequate written description when, for example, ‘the specification describes a reason to exclude the relevant [element].’ A reason to exclude an element could be

found in ‘statements in the specification expressly listing the disadvantages of using’ that element.” *Novartis Pharms. Corp.*, 38 F. 4th at 1016 (internal citations omitted).

The specification discloses the challenged limitation and authentication method where both devices use application specific authentication information that is not device specific (i.e., passwords): “One means of authentication, in some cases a password, is stored for authenticating the user on the first device, and a second means of authentication, possibly a different password, is stored to authenticate the user on the second device.” Ex. 2005, ¶90, Ex. 2009, ¶73-75. Further, the specification teaches the advantages and disadvantages of limiting the authentication process to non-device specific authentication information, which was a known concept to a POSITA and applied to all device attempting to access web applications. Ex. 2005, ¶92, Ex. 2009, ¶73-75. Applying *Navartis Pharms. Corp.*, the ’376 Patent sufficiently describes the negative limitation of narrowing first device authentication by excluding non-device specific authentication information. Not only does the specification disclose using this precise embodiment, but it also teaches the advantages and disadvantages of using non-device specific authentication.

Claim 28. Patent Owner further amended Substitute Claims 28 to specify that the second subset of information sensitive information sent to second device “**is only shared with the second device.**” The specification discloses a number of examples where the sensitive information is limited to only being shared with the second device.

Ex. 2005 ¶ 23-29, Ex. 2009, ¶¶ 78-79. Petitioner complains that this narrowing and negative limitation contradicts Rubin’s online poker embodiment because hole cards are shared with the first device once the game is completed. Pet Opp. at 2. Petitioner is incorrect. The hole cards are only shared when the hand is over and the hole cards no longer constitute sensitive information. Ex. 2009, ¶79.

In sum, the ’376 Patent specification reasonably conveys to those skilled in the art that Dr. Rubin had possession of the claimed subject matter for Substitute Claims 26, 28 and 41 as of the ’376 Patent filing date. Ex. 2009, ¶76, 80.

III. CLAIMS 32 AND 35 ARE NOT INDEFINITE.

Petitioner argues the term “*the information* displayed on the respective devices” is indefinite for lack of antecedent basis. Petitioner is incorrect.

A claim is indefinite if it does not inform, with “reasonable certainty,” a skilled artisan about the scope of the claimed invention. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014); MPEP s 2173.05(E) (“the failure to provide explicit antecedent basis for terms does not always render a claim indefinite. If the scope of a claim would be reasonably ascertainable by those skilled in the art, then the claim is not indefinite.”).

Here, the scope of the term “*the information* displayed on the respective devices” is easily ascertainable by a POSITA. The specification and original claim discuss “the information displayed on the respective devices” in the context of a

graphical indicator used to link the information displayed on the devices. The specification explains “the information” is the online poker table on the first device and the hole cards on the second device and the graphical indicator links the hand displayed on the first device to the hole cards on the second device. Ex. 2005, ¶26, Ex. 2009, ¶¶82-84. This is disclosed in the original claims where original claim 10 introduces the linking of “the information displayed on the respective devices” and original claim 11 states “the information linked at the second device comprises hole cards and the information linked at the first device comprises community cards in a hand in a game of poker.” Ex. 2005-029.

The scope of Substitute Claims 32 and 35 are reasonably ascertainable by a POSITA. Ex. 2009, ¶¶82-84. The information displayed on the respective devices refers to the display of the application running simultaneously on the two devices such as online poker game.

IV. PATENT OWNER’S THEREBY CLAUSE IS LIMITING.

Patent Owner further narrowed Claims 26 and 41 in two respects: the preamble makes clear the claims are for “*protecting information*” and the “if and only if” limitation further requires “*wherein the second subset of the information includes information not transmitted to the first device thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.*” Petitioner argues “protecting information” and “thereby protecting the

second subset of the information not transmitted to the first device from potential malware on the first device” are non-limiting. Petitioner is incorrect.

“[W]hen the ‘whereby’ clause states a condition that is material to patentability, it cannot be ignored in order to change the substance of the invention.” *Hoffer v. Microsoft Corp.*, 405 F.3d 1326, 1329 (Fed. Cir. 2005); *see also Amarr Co. Requester & Cross-Appellant v. Wayne-Dalton Corp. Pat. Owner & Appellant*, No. 2011-005126, 2011 WL 2491036, at *6 (B.P.A.I. June 20, 2011) (finding that “rather than simply providing the functional result of all of the features of the recited door, the ‘whereby’ clause recited in the claims adds to the patentability of the claims”).

Patent Owner’s “thereby” clause requiring the protection of the second subset of the information is an important element of the invention, and represents more than just an intended result. The ’376 Patent is entirely directed towards the protection of information in online transactions. Substitute Claims 26 and 41 recite a number of steps that, when taken together, can isolate information shared with an application users first and second devices. Ex. 2009, ¶¶ 85-86. However, if the information sent the second device is not ultimately protected from malware on the first device then the invention is not achieved. *Id.* Patent Owner’s thereby clause makes protecting of the second subset of information a requirement of the claims rather than an aspiration result of the practice of the steps. *Id.*

V. ZHA DOES NOT RENDER THE CLAIMS OBVIOUS.

A. Zha Fails to Disclose Several Key Limitations of Substitute Claim 26.

Claim 26[c]. *Zha* lacks any disclosure related to authenticating the user on the first and second device as claimed in 26[c]. *Zha* merely repeats in several places the user “logs in to microblog in the cellphone, the laptop computer and the desktop computer simultaneously.” *See e.g.*, Ex. 1004, Col.13:4-7. Accordingly, to meet this limitation, Petitioner argues that three separate references – *Kling*, *Lipetz* and *Gui* – all disclose the authentication process as claimed in 26[c], and a POSITA would have been motivated to combine these references with *Zha* and/or modify *Zha*. Petitioner arguments are without merit.

Kling fails to disclose the use of application specific authentication information that is not specific to a device and that is different for each device. Petitioner relied on *Kling*’s statement that when accessing one’s mobile phone one should “ideally” use a different password “then on the PC” (Ex. 1023, ¶18) but this does not disclose using two different passwords to authenticate with *Kling*’s banking application on the PC and mobile device. Ex. 2009, ¶91. It is common place for PCs and mobile devices to require their own passwords for login. Substitute Claim limitation 26[c] requires login to the “**application**” using two different passwords.

Moreover, there is no motivation to combine *Zha* with *Kling*. *Zha* permits any terminal (desktop, laptop, cellphone) to access any functional interface of the

application program. Ex. 1004, Col.12:34-13:11, 14:6-12, 15:56-58, 16:37-48; Ex. 2009, ¶ 92. Increasing the security and protection of the second subset of information not sent to the first device – the functional interfaces of the microblog home page – makes no sense, and unnecessarily complicates *Zha*, because the first device can simply change access permission and request access to any of the microblog functional interfaces. *Id.*

Lipetz similarly fails to disclose the use of application specific authentication information that is not specific to a device and that is different for each device. Ex. 2009, ¶93-96. Indeed, *Lipetz* does not contemplate logging into the same application at the same time on two different devices. *Id.* *Lipetz* merely discloses using different passwords to access different security levels within a single application on a single device. *Id.*

Similar to *Kling*, there is no motivation to combine *Zha* with *Lipetz*. Ex. 2009, ¶94-96. Petitioner argues a POSITA would have been motivated to enhance *Zha* against malware by adding two different passwords on the two devices. But *Zha*'s microblog is already fully accessible by one device at any time using a single password. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48. A POSITA would not be motivated to add a second different password on a second device to access *Zha*'s chat feature when the user could access the same chat feature on their first device with the same password. This is not logical and just hindsight reasoning by Petitioner to try

and piece together the various limitations of the '376 Patent.

The *Gui* reference also fails to disclose Substitute Claim limitation 26[c] as claimed. *Gui* is a new secondary reference asserted by Petitioner. *Gui* does not contemplate or disclose signing onto the same application on two different devices using two different passwords. Moreover, *Gui*'s "authentication system" outsources the authentication to a separate third-party "authentication system" server meaning none of the authentication of Substitute Claim limitation 26[c] is carried out by "the server." Ex. 1031, Col.7:27-32, Col.8:15-26, Ex. 2009, ¶¶97-99.

Gui's third-party "authentication system" discloses that ability to accept multiple types of passwords and authentication methods to authenticate the user, but the "service" (i.e., the banking application in the '376 Patent) "is typically unaware of the credential that was supplied by the user to the authentication system 210." Ex. 1031, Col.7:57-60. Substitute claims 26 and 41 both require that "the server" running "the application" makes the determination of whether the first and second devices are in possession of the user based on the user being logged into the "application using application specific authentication information that is not authentication information specific to a device" and the authentication information is different for each device. *Gui* authentication system issues a "user profile and/or ticket" to the users device which is in turn provides to the service for authentication. Ex. 2009, ¶¶97-99. In *Gui*, the server running the application (the "service") does not

know what type of authentication credentials were supplied to the authentication system. *Id.* Similarly, applying *Gui* to *Zha*, the server would also not know whether the authentication information used to login to two separate devices was different because the authentication system does not convey this information to the service. Ex. 1031, Col.7:57-60, Ex. 2009, ¶98.

Gui's authentication system also fundamentally does not address the security benefits Substitute Claims 26 and 41 achieve by requiring two different passwords. Ex. 2009, ¶99. Applying *Gui*'s system to *Zha*, a user is allowed to use the exact same password on the first device and second device to access the functional interfaces of *Zha*'s microblog. Substitute Claim limitation 26[c] requires that the passwords must be different. *Gui*'s "optional" different password teaches away from always requiring a different password on the second device. In attempting to combine *Gui* with *Zha*, if the first device has been compromised by malware, then the attacker can simply use the same password to log into *Zha*'s microblog on the second device. As Dr. Rubin explains in the '376 Patent, the benefit of requiring two different passwords protects against this very scenario. Ex. 2005 ¶ 90, Ex. 2009, ¶99.

Moreover, the foregoing example of the attacker compromising the first device in a *Gui/Zha* combination underscores why there's no motivation to modify *Zha* in light of *Gui* to require two different passwords when logging into *Zha*'s second device. Any attacker that gains access to *Zha*'s microblog on the first device already

has access to all of the functional interfaces of *Zha*’s microblog, and thus requiring a second different password on the second device adds nothing but additional operational complexity. Ex. 2009, ¶100.

In summary, *Gui*, *Kling* and *Lipetz* do not disclose the requirements of Substitute Claim limitation 26[c]. There is no motivation to combine these references with *Zha* because they do nothing to improve the security of *Zha*’s system.

Claim 26[d]. *Zha* fails to disclose the “protecting the second subset of the information not transmitted to the first device from potential malware on the first device.” *Zha* teaches providing the first device with access to all the same information available on the second device. Ex. 1004, Col.12:34-13:11, 14:6-12, 15:56-58, 16:37-48, Ex. 2009, ¶103-104.

Petitioner suggests that a *Zha* meets these limitations by arguing a user could configure *Zha* to have the private messages sent to their cellphone and thus protect that information from potential malware on their desktop. But this argument ignores *Zha*’s teaching that any terminal in *Zha* (the desktop, laptop and cellphone) can request access to any of the functional interfaces of *Zha*’s microblog. Ex. 1004, Col.12:34-13:11, 14:6-12, 15:56-58, 16:37-48, Ex. 2009, ¶104. An attacker that gains access to *Zha*’s first device, whether the desktop, laptop and cellphone, gains access to all of the functional interfaces of the microblog. Ex. 2009, ¶104.

Accordingly, *Zha* fails to disclose Substitute Claim limitation 26[d] “thereby

protecting the second subset of the information not transmitted to the first device from potential malware on the first device.”

B. Zha Fails To Disclose Substitute Claim 28.

Substitute Claims 28 requires the second subset of the information comprises sensitive information and *the sensitive information is only shared with the second device*. *Zha*’s private “messages” are by definition shared beyond the second device and therefore cannot meet this limitation. Ex. 2009, ¶¶110-12. Moreover, *Zha*’s private messaging is fully accessible on the first device, therefore *Zha* fails to only share sensitive information with the second device. *Id.*

Petitioner first contends that Patent Owner’s argument distinguishing *Zha* based on *Zha*’s disclosure of private messages between users contradicts every embodiment in the ’376 Patent. Pet. Opp. at 16-17. Petitioner argues the ’376 Patent’s “hole cards” are shared with every game participant and therefore the ’376 Patent discloses the same practice, but Petitioner is incorrect. The ’376 Patent only discloses the “hole cards” to the first device when the “hole cards” are longer considered “sensitive information.” Ex. 2005, ¶40, Ex. 2009, ¶111.

Petitioner’s second argument is that *Zha* only shares all the microblog interfaces in the *Zha* “single device” embodiment. This is incorrect. The entire *Zha* reference and every embodiment contemplates “at least” two devices. Ex. 2009, ¶112. As noted in the “Summary,” *Zha* discloses a method for “displaying an

interface” which includes “determining a first terminal and a second terminal.” Ex. 1004, Col.1:50-55. Further, Zha discloses a system for “displaying an interface” with “at least two terminals according to any of the foregoing possible implementations.” Ex. 1004, Col. 2:54-58. Zha **only** discloses two device embodiments and in all of these embodiments, any of the “at least two terminals” can request access to any of the functional interfaces of *Zha*’s microblog. Ex. 1004, Col.12:34-13:11, 14:6-12, 15:56-58, 16:37-48, Ex. 2009, ¶112. As a result, *Zha* teaches away from only sharing sensitive information with the second device because *Zha* discloses sharing its private message interface with any of the at least two terminals. Ex. 2009, ¶112.

C. *Zha* Fails To Disclose Substitute Claims 27, 29, 31, 32, 34-36, 37, 39, 40 and 41.

For the reasons stated in Patent Owner’s April 5, 2024 Revised Motion to Amend (Paper 22), *Zha* and its combinations fail to disclose Substitute Claims 27, 29, 31, 32, 34-36, 37, 39, 40 and 41.

VI. *KLING* DOES NOT RENDER THE CLAIMS OBVIOUS.

A. *Kling* Does Not Disclose the Limitations of Substitute Claim 26

Claim 26[d]. Substitute Claim 26, limitation [d] requires that BOTH devices be determined by the server to be logged in to the application prior to sending the first and second subsets of information. However, *Kling*’s figures 4 and 5 shows that this first subset of information is sent to the first device before the second device is logged into the application. Ex. 2023, Figs. 4, 5; *see also*, Ex. 2009, ¶¶133-135.

Accordingly, Kling fails to disclose this limitation.

Petitioner originally relied on *Tsushima* in attempt to satisfy the missing limitation but Petitioner's Opposition asserts a new reference, *Lim*, as purportedly disclosing the missing elements. Petitioner's reliance on *Lim* to combine with *Kling* fairs no better.

Petitioner asserts that *Lim* discloses "a user using two different authentication mechanisms (two different "application specific authentication information") from two different devices to access the application. Pet. Opp. (Paper 27) at 22. This is incorrect. *Lim* discloses authentication using only one device -- the mobile device. In *Lim*, a user connects with a "service server 300" (i.e., an online banking application) using the "user terminal 50." Ex. 1030 ¶ 28, Ex. 2009, ¶148. Thereafter, the remainder of the login process and authentication is carried out on *Lim*'s second device, the "mobile device 100" and is independent of *Lim*'s first device, the "user terminal 50." Ex. 1030 ¶¶ 29, 30-35, 38; Ex. 2009, ¶¶149-53.

Lim is clear that the first device does not authenticate: "That is, in the present invention, ***the user terminal 50 itself that will connect with the service server 300 does not perform authentication.***" Ex. 1030 ¶ 43. *Lim* further explains that "[i]n the present invention, the user terminal 50 only displays an identifier on a monitor screen in the authentication process, but does not become a principal agent of the authentication." Ex. 1030 ¶ 44. Accordingly, Petitioner has misinterpreted *Lim* as

disclosing a system where a user uses two different authentication mechanisms.

Claim 26[c]. *Kling* fails to disclose the use of application specific authentication information that is not specific to a device and that is different for each device. As discussed above, Petitioner relied on *Kling*'s statement that when accessing one's mobile phone one should "ideally" use a different password "then on the PC" (Ex. 1023, ¶18) but this does not disclose using two different passwords to authenticate with *Kling*'s banking application on the PC and mobile device. Ex. 2009, ¶¶159-61. Substitute Claim limitation 26[c] requires login to the "**application**" using two different passwords.

Petitioner attempts to fill *Kling*'s gap by arguing a POSITA would be motivated to modify *Kling* based on *Lim* to implement the use of application specific authentication information that is not specific to a device and that is different for each device. *Lim*, however, teaches away from requiring non-device specific authentication information for authentication because *Lim* specifically teaches the use of device specific authentication information for authenticating the "mobile device 100." Ex. 1030 ¶ 48 ("Here, the authentication information may be one or more of the phone number of the mobile terminal 100, a MAC address, USIM or SIM card information"). While *Lim* discloses use of non-device specific authentication information such as a username and password as one possible means for authenticating mobile device 100, *Lim* teaches away from limiting authentication

information to information that is not device specific. Finally, because *Lim* only discloses authenticating on one device (see discussion above), *Lim* fails to disclose authenticating on two devices using two different passwords.

B. *Kling* Does Not Disclose Substitute Claim 28.

Petitioner argues the “transaction confirmation web page information [Arrow #4]” comprises “sensitive information” and that “transaction confirmation web page information” is only shared with the user’s second device. Pet. Opp. 28. This argument fails because *Kling*’s “desired transaction” – the purportedly sensitive information shared only with the second device – has already been shared with the first device. Ex. 2009, ¶¶168-69. The desired transaction was generated by the user on the first device. *Id.* As noted above, Substitute Claim limitation 28[b] requires that “the sensitive information is only shared with the second device.” Accordingly, *Kling* teaches away from disclosing this limitation because *Kling* shares the “desired transaction” with both devices.

C. *Kling* Does Not Disclose Substitute Claims 27, 29, 31, 32, 34, 35, 39, 40, 41

For the reasons stated in Patent Owners April 5, 2024 Revised Motion to Amend (Paper 22), *Kling* and its combinations fail to disclose Substitute Claims 27, 29, 31, 32, 34, 35, 39, 40 and 41.

VII. TAKAHASHI DOES NOT RENDER THE CLAIMS OBVIOUS.

A. *Takahashi* Fails To Disclose Substitute Claim 26.

Claim 26[c]. Substitute Claim 26, limitation [c] requires “determining at the server” if both devices are accessible based on “the first user *being logged into the application*” using application specific authentication information. *Takahashi* specifically discloses logging in before authenticating which is the opposite sequence of Substitute Claim 26, limitation [c]. Ex. 2009, ¶¶183-85. In Figure 11, *Takahashi* authentication process occurs “after user logins.” Ex. 1007, Fig. 11. *Takahashi*’s paragraph 110 (describing Figure 11) discloses “processing after a registered user (that is, a user whose ID is registered) logins to the game server 20.” Ex. 1007, ¶110.

Petitioner contends *Takahashi*’s use of “login” means something different than its plain and ordinary meaning. Pet. Opp. at 23. Petitioner suggests the disclosure of “login” only relates to the initial step of a user submitting their credentials. *Id.* This argument is contradicted by *Takahashi*’s further disclosure that the users accessing of the game server is the same as the user logging in (Ex. 1007, ¶114) which demonstrates *Takahashi* doesn’t use the term “login” to refer only to the first step of submitting ones credentials. Ex. 2009, ¶¶183-85. *Takahashi* fails to disclose limitation 26[c] because it discloses authenticating after the user has logged in.

Takahashi also fails to disclose Substitute Claim limitation 26[c] because *Takahashi* specifically relies on device specific authentication information. Ex. 2009,

¶186. Patent Owner has further narrowed Substitute Claim limitation 26[c] to specifically exclude use of device specific authentication information. *Takahashi* discloses in paragraph 74 using identification information such as “a serial number of the mobile terminal” and therefore cannot meet this limitation. Ex. 1007, ¶74.

Petitioner suggests a POSITA would be motivated to modify *Takahashi* in light of *Gui* to add the missing limitations of 26[c]. Pet. Opp. (Paper 27) at 34-35. Petitioner is mistaken. *Gui* fails to fill the missing authentication disclosure for *Takahashi*. Ex. 2009, ¶¶221-24. *Gui*’s authentication is not carried out by the server, the type of authentication information used is unknown in each instance a device authenticates because it is not disclosed by the authentication service, and there is no requirement the authentication used to access both devices is different. *Id.*

Gui’s authentication system also undermines the security the security benefits of Substitute Claims 26 and 41 achieve by requirement of two different passwords. Ex. 2009, ¶224. Indeed, combining *Gui* with *Takahashi* reduces the security of *Takahashi*’s authentication scheme because *Takahashi* already requires use of two different passwords where *Gui* does not. *Id.* An attacker that gains access to the login information on the first device using *Gui*’s authentication system can use the same login information on the second device.

Petitioner suggests a POSITA would have been motivated to modify *Takahashi* consistent with *Gui* to make authentication easier on different types of

devices by allowing different authentication credentials. Pet. Opp. at 35. *Takahashi* already discloses a two password scheme where the mobile device automatically uses device specific “identification information” to authenticate the second device which is an even easier authentication process disclosed by *Gui* which still requires the user to input their authentication credentials. Compare Ex. 1007 ¶110 (*Takahashi*) with Ex. 1030, Col. 2:20-47 (*Gui*). There is no motivation to modify *Gui* where *Gui* discloses a less secure and less “user friendly” authentication system than the system already disclosed by *Takahashi*.

Claim 26[d]. *Takahashi* fails to disclose this limitation. *Takahashi* teaches providing the first device with access to all the same information on the second device. Ex. 2009, ¶¶188-89. Petitioner continues to point at *Takahashi*’s two-device embodiments as disclosing “protecting the second subset of information” but ignores that the *Takahashi* reference as a whole teaches away from protecting the second subset of information from malware on the first device.

B. Takahashi Fails to Disclose The Limitations of Remainder of the Substitute Claims.

Takahashi fails to disclose the limitations of Substitute Claims 27-35 and 37-41. See RMTA (Paper 22) at 23; Ex. 1009, ¶¶190-219.

VIII. ZHA, TAKAHASHI AND TSUSHIMA ARE NOT ANALOGOUS ART

Zha, *Takahashi* and *Tsushima* are not analogous art under controlling Federal Circuit caselaw. See RMTA (Paper 22) at 24; Ex. 1009, ¶¶225-247.

Dated: June 14, 2024.

/Robert S. McArthur/

Robert S. McArthur, Esq.
Registration No. 45,674
VASQUEZ BENISEK & LINDGREN LLP
1550 Parkside Drive, Ste 130
Walnut Creek, CA 94596
Main Telephone (925) 637-4250
Direct Telephone (415) 699-0630
Main Facsimile (925) 403-0900
mcarthur@vblaw.com
Counsel for Patent Owner

CERTIFICATE OF FILING AND SERVICE

I hereby certify that a true and correct copy of the foregoing PATENT OWNER'S REPLY IN SUPPORT OF REVISED MOTION TO AMEND is being filed electronically via P-TACTS and served on counsel for Petitioner by electronic mail this 14th day of June, 2024 as follows:

R. William Beard, Jr. (wbeard@sgbfirm.com)
Brian C. Banner (bbanner@sgbfirm.com)
SLAYDEN GRUBERT BEARD PLLC
401 Congress Avenue, Suite 1650
Austin, Texas 78701
litigation@sgbfirm.com

Dated: June 14, 2024

/Robert S. McArthur/
Robert S. McArthur, Esq.
Registration No. 45,674
VASQUEZ BENISEK & LINDGREN LLP
1550 Parkside Drive, Ste 130
Walnut Creek, CA 94596
Main Telephone (925) 637-4250
Direct Telephone (415) 699-0630
Main Facsimile (925) 403-0900
mcarthur@vblaw.com
Counsel for Patent Owner