

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 REVISED NON-CONTINGENT
MOTION TO AMEND U.S. PATENT NO. 9,064,376**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PRELIMINARY GUIDANCE FROM THE BOARD	1
III.	THE REQUIREMENTS OF 37 C.F.R. § 42.121 ARE SATISFIED	1
A.	Substitute Claims are Provided in a Claims Listing.....	1
B.	The Number of Substitute Claims are Reasonable.....	1
C.	The Amendments are Responsive to the Grounds at Issue	2
D.	The Amendments are Non-Broadening.....	2
E.	The Amendments Have Written Description Support.....	2
IV.	PERSON OF ORDINARY SKILL IN THE ART (POSITA).....	7
V.	THE PROPOSED SUBSTITUTE CLAIMS ARE PATENTABLE OVER THE INSTITUTED GROUNDS AND ART	7
A.	<i>Kling</i> Does Not Disclose the Limitations of the Substitute Claims.	7
1.	Substitute Claim 26, Limitation [d].....	8
2.	Substitute Claim 28	10
3.	Substitute Claim 30	11
4.	Substitute Claims 27-29, 31, 34, 40-41	12
B.	<i>Zha</i> Does Not Disclose Substitute Claims 26-32, 34-37, 39-41	12

1.	Substitute Claim 26, Limitation [c]	13
2.	Substitute Claim 28	16
3.	Substitute Claims 27-32, 34-37, 39-41	17
C.	<i>Takahashi</i> Does Not Disclose Substitute Claims 26-35 and 37-41	18
1.	Substitute Claim 26, Limitation [c]	19
2.	Substitute Claim 27	21
3.	Substitute Claim 28	22
4.	Substitute Claim 33	23
5.	Substitute Claims 27-35, and 37-41	23
D.	<i>Zha</i> and <i>Takahashi</i> Are Not Analogous Art.....	24
VI.	CONCLUSION	25

TABLE OF AUTHORITIES

CASES

<i>Airbus S.A.S. v. Firepass Corp.</i> , 941 F.3d 1374 (Fed. Cir. 2019).....	24
<i>Aqua Prods., Inc. v. Matal</i> , 872 F.3d 1290 (Fed. Cir. 2017)	7

STATUTES

37 C.F.R. § 42.121(a)(3)	1
37 C.F.R. § 1.121(c)(2)	1

LIST OF EXHIBITS

Exhibit No.	Description
2008	Second Declaration of Patrick Traynor, Ph.D. in support of Patent Owner's Revised Non-Contingent Motion to Amend U.S. Patent No. 9,064,376

I. INTRODUCTION

Patent Owner Dr. Aviel D. Rubin (“Rubin” or “Patent Owner”) submits this Revised Non-Contingent Motion to Amend (“Revised Motion”) to request amendment of challenged claims 1-5, 9-10, 12-17, and 23-25 of U.S. Patent No. 9,064,376 (“the ’376 Patent”) in order to provide further clarification of the invention set forth therein. Pursuant to 35 U.S.C. § 316(d)(2) and Notice, 84 Federal Registration at 9497, Patent Owner submits this Revised Motion proposing new substitute claims 26-41 (the “Substitute Claims” set forth in Appendix A) for original claims 1-5, 9-10, 12-17, and 23-25 of the ’376 Patent.

II. PRELIMINARY GUIDANCE FROM THE BOARD

Patent Owner requests further preliminary guidance from the Board on this Revised Motion pursuant to the Motion to Amend (MTA) Pilot Program, initiated on March 15, 2019. 84 Fed. Reg. 9497; Scheduling Order, Paper 11 at 4-6.

III. THE REQUIREMENTS OF 37 C.F.R. § 42.121 ARE SATISFIED

A. Substitute Claims are Provided in a Claims Listing

The claim listing is attached as Appendix A. The claim listing cancels original claims 1-5, 9-10, 12-17, and 23-25 and includes Substitute Claims 26-41. The Substitute Claims include annotations pursuant to 37 C.F.R. § 1.121(c)(2).

B. The Number of Substitute Claims is Reasonable

Pursuant to 37 C.F.R. § 42.121(a)(3), the number of Substitute Claims is

reasonable. Patent Owner proposes 16 non-contingent Substitute Claims (claims 26-41), each of which corresponds to the 16 Challenged Claims (original claims 1-5, 9-10, 12-17, and 23-25).

C. The Amendments are Responsive to the Grounds at Issue

The proposed Substitute Claims in this Revised Motion are responsive to the Grounds at issue in this proceeding because they further distinguish the claims from the art of record. For instance, the Substitute Claims provide clarity by adding limitations relating to the disclosure of the '376 Patent for (i) using authentication information not specific to a device for logging into the application and (ii) sharing “sensitive information” only with the second device. For these reason, and as further explained below, the Substitute Claims are patentable over the instituted Grounds.

D. The Amendments are Non-Broadening

The Substitute Claims do not seek to enlarge the scope of the original claims. Dependent Substitute Claims 27-40 all depend from Substitute claim 26, and thus are narrowed by the narrowing amendment to Substitute claim 26. Substitute dependent claims 27-40 also include all of their original limitations.

E. The Amendments Have Written Description Support

Each of the proposed Substitute Claims 26-41 have written description support in the U.S. Patent Application No. 14/444,995 (“the '995 App.”) (now U.S. Patent No. 9,064,376)(Exhibit 2005). As shown in the table below, each limitation of the

Substitute Claims is disclosed in the specification and/or figures of the '995 App.

The **bolded** text and **bolded strikethrough** text in the “Claim Element” box represents claim language added or deleted as part of this Revised Motion.

Paragraphs citations for written description that are **bolded** and underline represent additional written description support for the additional changes to the Substitute Claims 26-41 made in this Revised Motion. Paragraphs that are **bolded** but not underlined represent written description support identified in the Original Motion that also supports the additional changes made in this Revised Motion.

Claim	Claim Element of Substitute Claim	'995 App. (Ex. 2005)
[26 Pre]	A method for protecting information by transmitting information to multiple electronic devices, the method comprising:	¶2, ¶¶18-19, <u>¶20</u> ¶¶23-25, <u>¶55</u> ; <u>¶61</u> ; <u>¶¶63-65</u> , <u>¶78</u> ; <u>¶81</u> , <u>¶83</u> , <u>¶93</u> ;
[26a]	electronically storing a set of information at a server;	Fig. 5-6; ¶25; ¶38; ¶39; ¶¶89-90;
[26b]	identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	¶¶23-28; ¶38;
[26c]	determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not authentication information specific to a device at both the first and second devices, wherein the	Fig. 10; ¶26; ¶33; ¶75; <u>¶83</u> ; <u>¶89</u> ; <u>¶90</u> ; <u>¶92</u> ;

	application specific authentication information used on the first device is different from the application specific authentication information used on the second device.	
[26d]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, 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.	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; Fig. 7; Fig. 9; Fig. 10; ¶20; ¶¶23-29 ¶¶33-34; ¶55; ¶58; ¶61; ¶¶63-65; ¶78; ¶81; ¶82; ¶83; ¶93;
[27]	The method of claim 26, further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.	¶24; ¶¶38-39; ¶45; ¶48;
[28a]	The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and	¶¶30-32;
[28b]	the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.	¶¶23-26; ¶29; ¶¶30-32; ¶35; ¶57; ¶63; ¶78; ¶82;
[29]	The method of claim 26, wherein the information received at the second device is more sensitive than the information received at the first device.	¶24; ¶¶30-32; ¶35; ¶57; ¶78;
[30]	The method of claim 28, further comprising: determining if connectivity between the server and the second device has been disrupted; and providing a notification by the application on the second device that the connectivity has been disrupted.	¶33; Claim 5 (p.28)
[31]	The method of claim 26, wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.	Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35;
[32]	The method of claim 26, further comprising displaying a graphical identifier on the first device and a	¶45; ¶48;

	corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.	
[33]	The method of claim <u>26</u> , wherein the information received at the second device is a user's private cards in an online card game.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶¶25-26; ¶31; ¶45; ¶48;
[34]	The method of claim <u>26</u> , wherein the a display on the first device is being viewed exclusively by a first user and a display on a second device is also being viewed exclusively by the first user.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶¶25-26; ¶31; ¶35; ¶39; ¶45; ¶48; ¶57; ¶65; ¶78;
[35]	The method of claim <u>30</u> , wherein, neither the first subset of information nor the second subset comprise a two factor authentication code, and, further comprising 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.	¶45; ¶48;
[36]	The method of claim <u>26</u> , wherein the server is a proxy server configured to relay communications from an application server to the first and second devices wherein the proxy server emulates a client to the application server.	¶50; ¶52;
[37]	The method of claim <u>26</u> , further comprising configuring the server for managing an online game, and wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, wherein the first electronic device is primarily used to play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.	¶23; ¶25; Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35; Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶¶25-26; ¶31; ¶45; ¶48;
[38]	The method of claim <u>37</u> , wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶¶25-26; ¶31; ¶45; ¶48;
[39]	The method of claim <u>26</u> , further comprising electronically storing at the server a parameter	¶¶25-26; ¶31; ¶¶33-34; ¶35;

	indicating whether subsets of the information are to be divided between two or more devices.	
[40]	The method of claim 26, wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.	¶¶20-23; ¶55; ¶57; ¶¶77-78;
[41pre]	A system for protecting information by transmitting information to multiple electronic devices, the system comprising:	¶2; ¶¶18-19; <u>¶20</u> ; ¶¶23-25; <u>¶55</u> ; <u>¶61</u> ; <u>¶¶63-65</u> ; <u>¶78</u> ; <u>¶81</u> ; <u>¶83</u> ; <u>¶93</u> ;
[41a]	an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶¶89-90;
[41b]	a processor device programmed for:	¶81; ¶98; ¶¶101-102;
[41c]	identifying a first subset of the information and identifying a second subset of the information;	¶23-28; ¶38;
[41d]	determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not authentication information specific to a device at both the first and second devices wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device;	Fig. 10; ¶26; ¶33; ¶75; <u>¶83</u> ; <u>¶89</u> ; <u>¶90</u> ; <u>¶92</u> ;
[41e]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device thereby protecting the second subset of the	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; <u>Fig. 7</u> ; <u>Fig. 9</u> ; <u>Fig. 10</u> ; <u>¶20</u> ; ¶¶23-29; ¶¶33-34; <u>¶55</u> ; ¶58; <u>¶61</u> ; <u>¶¶63-65</u> ; <u>¶78</u> ;

	information not transmitted to the first device from potential malware on the first device.	<u>¶81; ¶82; ¶83; ¶93;</u>
--	--	-----------------------------------

IV. PERSON OF ORDINARY SKILL IN THE ART (POSITA)

Patent Owner agrees with Petitioner that a POSITA would have two years of professional experience in the field of (i) computer and security, and/or (ii) network design and security. Ex. 2004, ¶39. Patent Owner objects to Petitioner’s use of the catchall “or other relevant industry experience” as vague and unhelpful. Ex. 2004, ¶39.

V. THE PROPOSED SUBSTITUTE CLAIMS ARE PATENTABLE OVER THE INSTITUTED GROUNDS AND ART.

The Substitute Claims distinguish the cited references relied upon in the Board’s institution decision with respect to independent claims 1 and 25 (corresponding to Substitute Claims 26 and 41). Patent Owner does not bear the burden of proving the patentability of Substitute Claims 26-41. *See Lectrosonics*, Paper 15 at 3-4; *Aqua Prods., Inc. v. Matal*, 872 F.3d 1290, 1295-96, 1327 (Fed. Cir. 2017) (*en banc*). Rather, Petitioners must prove unpatentability by a preponderance of the evidence. *See Lectrosonics*, Paper 15 at 4. Nonetheless, Patent Owner provides the following comments in support of the Substitute Claims and in response to the Board’s Preliminary Guidance (“PG”) and Petition’s February 23, 2024 Opposition (“PO”).

A. Kling Does Not Disclose the Limitations of the Substitute Claims.

In response to Patent Owners Original Motion, Petitioner’s cited *Kling* as § 103 prior art. *Kling* is old art cited in Dr. Rubin’s IDS and fails to disclose several limitations across Substitute Claims 26-41. For Substitute Claims 26 and 41, *Kling*

fails to disclose authentication requirements of 26[c] and the “if and only if” limitation of 26[d]. *Kling* further fails to disclose “sensitive information” under 28[b] as construed by the Board. And *Kling* fails to disclose providing notification of connectivity as required by Substitute Claims 30 and 35.

1. Claim 26, Limitation [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. Petitioner identifies “enter desired transaction 407” as corresponding to the “first subset of information” in Substitute Claim 26. Ex. 2027, ¶87. 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. 2008, ¶¶54-55. Accordingly, *Kling* fails to disclose this limitation.

Anticipating this gap, Petitioner argues the “if and only if” limitation is generally known to a POSITA based on *Tsushima* (Ex. 1027, ¶¶100-104), and that a POSITA would have been motivated to modify *Kling* to add this limitation because of “*Kling*’s goal of preventing malware breaches in a banking application[s].” Ex. 1027, ¶103. Petitioner is incorrect. As explained by Dr. Traynor, adding the “if and only if” step to *Kling* (i.e., requiring both devices to be logged into the application before sending the first subset of information to the first device) does nothing to improve *Kling*’s security. Ex. 2008, ¶¶57-60. Adding the “if and only if” step would

allow *Kling* to intercept the attempted malware hijack in Figure 5 as it did previously, but it would not prevent malware on the first device from accessing all the confidential information exposed to the first device. Ex. 2008, ¶¶57-59. The same information is sent to both devices and the second device’s separate “authorization” step is still required to approve the requested transaction. *Id.* Indeed, as explained by Dr. Traynor, adding the “if and only if” limitation to *Kling* provides no extra security but disrupts the operation of *Kling*’s banking application. Ex. 2008, ¶¶61, 64-65.

Kling does not disclose the “if and only if” limitation of Substitute Claim 26[d] and a POSITA would have no motivation to modify *Kling* to add the limitation.

Limitation [c]. Substitute Claim 26, limitation [c] requires being logged into “the application using application specific authentication information that is not authentication information specific to a device . . . wherein the application specific authentication information . . . is different” for both devices. *Kling* fails to disclose multiple aspects of this limitation.

First, *Kling* discloses using authentication information specific to a device, which is contrary the claim. *Kling* initiates a “secondary authentication request” to a “mobile device . . . that the user has previously registered with the bank server.” Ex. 1023, ¶17. *Kling*’s lookup of a registered mobile device for secondary authentication is clearly use of authentication information specific to a device. Ex. 2008, ¶67.

Second, Petitioner argues *Kling* discloses using two different passwords on the first and second devices for logging into the application, and that this disclosure matches Substitute Claim limitation 26[c]. Petitioner mischaracterizes *Kling*. *Kling* discloses that “[t]ypically the user would be prompted ***to log into the mobile device***, ideally using a different password than on the PC.” Ex. 2023, ¶118; Ex. 2008, ¶¶69-71. *Kling*’s disclosure directs the user to log into their mobile device with a different password, and not ***the application*** which is what Substitute Claim 26[c] requires. *Id.*

In summary, *Kling* does not disclose (i) using application specific authentication information that is “not authentication information specific to a device” or (ii) using two different passwords to log into ***the application***.

2. Substitute Claim 28. Substitute Claim 28, limitation [b] requires that “the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.”

The Board’s Preliminary Guidance applied the plain and ordinary meaning to “sensitive information.” PG at 20, Ex. 3002. In response, Patent Owner has further amended Substitute Claim 28 to require that the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device. *Kling* does not disclose sensitive information sent to the second device. Moreover, the information Petitioner argues is sensitive information sent to the second device is also shared with the first device in violation of the claim.

In particular, Petitioner identifies “enter OK or Cancel” as the “sensitive information” sent to the second device. Ex. 2027, ¶111. The information – “enter OK or Cancel” – on its face is not “sensitive information” as construed by the Board. Ex. 2008, ¶78. The “enter OK or Cancel” message delivered by Kling is a prompt that requires the user to take an action – either approve or cancel a transaction. The information itself (“enter OK or Cancel”) is not confidential as construed by the Board, as its disclosure outside the second device would not be harmful. *Id.*

Petitioner further argues that Kling’s transmission of the “desired transaction” to the mobile device is also sensitive information. Ex. 2027, ¶112. This argument fails because the “desired transaction” information, even if sensitive information, has already been shared with the first device by the time it is sent to the second device. Ex. 2008, ¶79. Substitute Claim 28[b] requires that sensitive information is only shared with the second device, therefore Petitioner’s argument fails.

3. Substitute Claim 30. Substitute Claim 30 requires that “determining if connectivity between the server and the second device has been disrupted; and providing a notification on the second device that the connectivity has been disrupted.” *Kling* does not disclose this limitation.

Moreover, there would be no motivation to modify *Kling* to add this functionality. As explained by Dr. Traynor, *Kling*’s connectivity with the second device is momentary and for the limited purpose of providing secondary

authentication of a transaction carried out on the first device. Ex. 2008, ¶¶83-84. The '376 Patent by comparison, describes several embodiments including online poker that require persistent connection throughout the interaction otherwise the entire session is terminated. Ex. 2005, ¶¶31-32; Ex. 2008, ¶¶83-84.

4. Substitute Claims 27-29, 31, 34, 40-41.

Substitute Claims 27-29, 31, 34 and 40 all depend from Substitute Claim 26 and therefore for the reasons *Kling* does not disclose the limitations of Substitute Claim 26, *Kling* also fails to disclose the limitations of Substitute Claims 27-29, 31, 34 and 40. Further, Substitute Claims 30 and 35 depend from Substitute Claims 28 and therefore for the reasons *Kling* does not disclose the limitations of Substitute Claim 28, *Kling* also fails to disclose the limitations of Substitute Claims 30 and 35. Finally, Substitute Claim 41 is the system claim of Substitute Claims 26 and contains essentially the same limitations as Substitute Claims 26. *Kling* fails to disclose the limitations of Substitute Claims 41 for the same reasons it fails to disclose the limitations of Substitute Claims 26.

B. *Zha* Does Not Disclose Substitute Claims 26-32, 34-37, 39-41.

As discussed below, *Zha* is not analogous art to the '376 Patent. At based, *Zha* discloses reducing network traffic when a user logs into an application (i.e., a microblog like Facebook) from more than one device simultaneously. *Zha* sends only a portions of the microblog to each device so that extra data is not extraneously

transmitted to each device. In *Zha*, when a user logs into Facebook with a single device (i.e., not simultaneously with another device) that user gets full access to all interfaces of the microblog. Ex. 1004, Col. 14:6-12. This is the opposite of the '376 Patent which requires log in from two devices before either device receives subsets of information. In *Zha*, only when the user decides to login to Facebook simultaneously with a second device does *Zha*'s network traffic reduction commence by sending different functional interfaces to different devices. Ex. 1004, Col. 2:15-19. Further, in *Zha*, any terminal can request and change its assigned functional interface and thus receive different functional interfaces (i.e., the desktop that was sent the homepage requests the chat app, or the cellphone sent the chat app requests the game interface). Ex. 1004, Col. 15:56-58, 16:37-48; Ex. 2008, ¶¶99-100. *Zha*'s microblog allows one password to access all the interfaces of the microblog on a single device. Ex. 2008, ¶¶99-100.

1. Substitute Claim 26, Limitation [c]. Substitute Claim 26, limitation [c] requires “*using application specific authentication information that is not authentication information specific to a device . . . wherein the application specific authentication information . . . is different*” for the two devices. *Zha* does not mention or disclose the use of authentication information that is “application specific” and that the application specific authentication information is different for determining login to the application at the first and second devices. Ex. 2004, ¶52.

This is not surprising given the objective of *Zha* is to reduce network traffic when a user is logged into a microblog like Facebook on multiple devices.

Petitioner concedes *Zha*'s missing disclosure, but argues using two different passwords for logging into an application on different devices was generally known by a POSITA (citing *Kling* and *Lipetz*). As noted previously, *Kling* discloses using device specific authentication information for logging into the second device. *See* pp. 9-10. Further, *Kling* only mentions it would be beneficial to use a different password for *the mobile device* and the PC, but *Kling* does not disclose using a different password for logging into *the application* on the second device. *See* p. 10.

Even if one assumed *Kling* disclosed using two different passwords on two different devices to log into the application, combining *Kling* with *Zha* would only make sense if *Zha* already required two different passwords on a single device to access the different interfaces for heightened security. Ex. 2008, ¶¶96-101. Petitioner argues a POSITA would have been motivated to enhance *Zha* against malware by adding two different password on the two devices. Ex. 2027, ¶¶145-46, 151-53. But *Zha*'s microblog is already fully accessible by one device at anytime using a single password. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48; Ex. 2008, ¶¶96-101. 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 a classic

example of impermissible hindsight analysis. Ex. 2008, ¶¶99-101.

Petitioner's reliance on *Lipetz* is similarly misplaced. *Lipetz* discloses a software security strategy for assigning a user multiple passwords that correspond with multiple security levels within an application on a single device. Ex. 1025, Col.1:6-10, 6:10-14. A user will enter a new different password on the same device if the user wants to change their level of security access. *Id.*; Ex. 1025, Col. 8:52-62. The '376 Patent teaches using two separate passwords on two separate devices to log in simultaneously to a single application, which will not transmit information until both devices are authenticated and logged in. Ex. 2008, ¶¶97-101. *Lipetz* disclosure of using two different passwords on one device to gain different security level access at different times within one application does not teach or disclose using two different passwords on two devices to simultaneously log into one application before that application will transmit protected information. *Id.*

Applying *Lipetz* to *Zha* presents the same flaws as combining *Kling* with *Zha*. Ex. 2008, ¶100. *Zha*'s microblog already permits the first device to fully access any of the microblog's functional interfaces (i.e., homepage, private chat or games) using a single password. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48; Ex. 2008, ¶¶98-101. Adding a second password for the user to remember on a second device offers no heightened security because the user protected information is already fully accessible on the first device with one password. Ex. 2008, ¶101.

In sum, *Kling* and *Lipetz* do not disclose using application specific authentication information that is not authentication information specific to a device . . . wherein the application specific authentication information used is different for both devices. As discussed above, even if *Kling* and/or *Lipetz* disclosed limitation 28[c], a POSITA would not be motivated to modify *Zha* and add this limitation.

Preamble and limitation [d]. Dr. Rubin has further modified Substitute Claim 26 in the preamble and limitation [d] to make clear that the practice of the claim enhances data protection. In particular, the preamble provides that the method is for “protecting information.” Limitation [d] in the body of the claim was modified to add “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first.”

Zha does not meet either of these limitations. First, *Zha* does not protect information by transmitting information to multiple devices. *Zha* does not disclose protecting information at all, but more importantly, *Zha* teaches sharing that same information with a single device. Ex. 2008, ¶¶106-107. Second, *Zha* does not disclose 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 on the second device. Ex. 2008, ¶¶106-07 Accordingly, *Zha* does not disclose the preamble or the revised limitation [d].

2. 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*. Dr. Rubin has further narrowed this claim by specifying “sensitive information is only shared with the second device.” The Board’s Preliminary Guidance accepted Petitioner’s argument that *Zha*’s private messages on the messaging app could constitute sensitive information. PG at 21. However, private “messages” are by definition shared beyond the second device and therefore cannot meet this limitation. Ex. 2008, ¶¶109-13. As noted above, Moreover, *Zha*’s microblog is fully accessible on the first device, including the private chat app. Thus, *Zha* teaches sharing the private messages (sensitive information) with the first device as well as sending private messages (sensitive information) to any number of other devices that are not second device. *Zha* fails to disclose the limitations of Substitute Claim 28.

3. Substitute Claims 27-32, 34-37, 39-41.

Substitute Claims 27-32, 34-37, 39 and 40 all depend from Substitute Claim 26. For the reasons *Zha* does not disclose the limitations of Substitute Claim 26, *Zha* also fails to disclose the limitations of Substitute Claims 27-32, 34-37, 39 and 40. Further, Substitute Claims 30 and 35 depend from Substitute Claims 28. For the reasons *Zha* does not disclose the limitations of Substitute Claim 28, *Zha* also fails to disclose the limitations of Substitute Claims 30 and 35. Finally, Substitute Claim 41

is the system and contains essentially the same limitations as Substitute Claims 26. *Zha* fails to disclose the limitations of Substitute Claims 41 for the same reasons it fails to disclose the limitations of Substitute Claims 26.

In summary, *Zha* alone, or in combination with knowledge of POSITA or Petitioner's other cited references, fails to disclose the limitations of Substitute Claims 27-32, 34-37, 39-41.

C. Takahashi Does Not Disclose Substitute Claims 26-35 and 37-41.

Takahashi relates to “a technique for controlling game progress with a communications terminal of a user via a communications network.” Ex. 1007, ¶2. *Takahashi* states that the object of the invention is directed to a “game control device, a non-transitory computer readable recording medium, a game control method, and a game control system that allows a variety of types or forms of games by use of a plurality of communications terminals.” Ex. 1007, ¶6. The “problem” identified by *Takahashi* is that a user of a social network games uses a “mobile communication terminal irrespective of where the user is” thus “it is difficult to realize a variety of types or forms of games on the assumption that the user uses a single communication terminal.” Ex. 1007, ¶5.

Similar to *Zha*'s microblog, *Takahashi*'s system works with an application whether carried out on one device or two devices. Ex. 2008, ¶150. Similar to *Zha*, *Takahashi* is designed to share all the applications information with the first device

when played on the first device, and only separates information when a second device is added. *Id.*

1. Substitute Claim 26, Limitation [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. 2008, ¶¶134-36. 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. Finally, *Takahashi*’s paragraph 14, which describes Figure 12, demonstrates *Takahashi* applies a plain and ordinary meaning to login. Ex. 2008, ¶¶134-36. In paragraph 14, *Takahashi* equates accessing the game server as the same thing as logging in. Ex. 1007, ¶114 (“an access is received to the game server 20 (that is, a user logins)”); Ex. 2008, ¶¶134-36.

Petitioner contends *Takahashi*’s use of “login” means something different than its plain and ordinary meaning. PO at 23. Petitioner suggests the disclosure of “login” only relates to the initial step of a user submitting their credentials. *Id.* But this argument is contradicted by *Takahashi*’s further discloser 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. 2008, ¶¶134-36. Accordingly, *Takahashi* fails to disclose Substitute Claim limitation 26[c] because *Takahashi* discloses authenticating the user 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. 2008, ¶137. The Board's Preliminary Guidance found that "use of 'identification information' that is unique to each mobile terminal" appears to correspond with "application specific authentication information." PG at 26. Dr. Rubin 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.

The Board's Preliminary Guidance suggests that it would be reasonable to combine *Takahashi* with *Kling*'s multiple/different passwords to improve *Takahashi*'s security against malware. PG at 26. However, combining *Takahashi* with *Kling* would still fail to disclose Substitute Claim 26[c] and not improve *Takahashi*'s security. As discussed above (pp. 9-10), *Kling* discloses using device specific authentication information for the second device similar to *Takahashi* disclosure in paragraph 74. Moreover, the "different" password *Kling* refers to is the password to

the “mobile device,” not the password for logging into the application on the mobile device as claimed. Further, there would be no motivation to combine *Takahashi* with *Kling* to increase security. *Takahashi* already discloses using authentication information that is different on the two devices. Ex. 1007, ¶110. As described in paragraph 110, *Takahashi* discloses using a user name and password for authenticating the PC, and “identification information” such as a device ID for the mobile device. *Id.* That is what *Kling* already discloses, and which still fails to meet limitation [c]. Ex. 2023, ¶17; Ex. 2008, ¶¶138-40.¹

Preamble and limitation [d]. As discussed above, Dr. Rubin has further modified Substitute Claim 26 in the preamble and limitation [d] to require enhancing data protection. *Takahashi* fails to disclose these limitation. *Takahashi*’s system that allows for single device operation and switching between one and two devices, teaches away for protecting the second subset of information from potential malware on the first device. Ex. 2008, ¶141-43.

2. Substitute Claim 27. Substitute Claims 27 requires “transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the

¹ The ’376 Patent teaches that if this type of authentication method is used it will limit the user to a specific device. Ex. 2005, ¶92. Accordingly, the ’376 Patent’s avoidance of device specific information is not to improve security by using two different passwords as the Board suggests, but to enhance the user experience. Ex. 2008, ¶68.

server.” *Takahashi* fails to disclose this limitation because *Takahashi* discloses sending information to the first and second devices that is different:

“In this case, the HTML data (second game data) transmitted to the main-terminal and the HTML data (first game data) transmitted to the sub-terminal are different each other.”

Ex. 1007, ¶107; *see also* Ex. 1007, ¶116. Because Substitute Claim 27 requires that at least a portion of the first subset of information be sent to the second device, *Takahashi* fails to disclose this limitation. Ex. 2008, ¶¶144-46.

3. Substitute Claim 28. Substitute Claim 28 specifies that “the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.”

Petitioner argues that the user’s “game results” could constitute (i.e., number of fish caught in Fig. 8) sensitive information. Ex. 1027, ¶210. Game results for a social fishing game meant to be played with friends does not meet the Board’s construction of sensitive information. Ex. 2008, ¶¶151-53. Moreover, *Takahashi* teaches away from sharing sensitive information with only the second device. The “game results” in *Takahashi*’s single device embodiment are by definition shared with the first device. Ex. 2008, ¶153. In *Takahashi* single device embodiment where a second device is added, the game results start on the first device and then may be sent to the second device. Ex. 2008, ¶¶152-53.² Similarly, *Takahashi*’s two device

² For example, in *Takashi* the user may access the game via a single terminal where

embodiments contemplate disconnecting the second device and continuing the game on the first device whereby any purported “sensitive information” such as “game results” is sent to the first device. Ex. 1007, ¶143, Fig. 20; Ex. 2008, ¶153.

4. Substitute Claim 33. Substitute Claim 33 requires that “information received at the second device is a user’s private cards in an online card game.”

Takahashi does not disclose this limitation, and Petitioner provides no evidence that *Takahashi* in combination with any other reference discloses sending the user’s private cards to the second device in an online card game.

5. Substitute Claims 27-35 and 37-41.

Substitute Claims 27-35 and 37-40 all depend from Substitute Claim 26. For the reasons *Takahashi* does not disclose the limitations of Substitute Claim 26 it also fails to disclose the limitations of Substitute Claims 27-35 and 37-40. Further, Substitute Claims 30 and 35 depend from Substitute Claims 28. For the reasons *Takahashi* does not disclose the limitations of Substitute Claim 28 it also fails to disclose the limitations of Substitute Claims 30 and 35. Finally, Substitute Claim 41

all the game information is delivered before adding a second terminal:

Note that there is a case in which a user starts the game by accessing first through a single communication terminal (mobile terminal 10, for example) and then accesses through the other communication terminal (PC 12, for example) as well in the middle of the game. . . . The game server 20 then switches transmission destination of the HTML data for displaying a new web page from the mobile terminal 10 to the PC 12.

Ex. 1007, ¶120.

is the system claim and contains essentially the same limitations as Substitute Claims 26. *Takahashi* fails to disclose the limitations of Substitute Claims 41 for the same reasons it fails to disclose the limitations of Substitute Claims 26.

D. Zha and Takahashi Are Not Analogous Art

The Board’s Preliminary Guidance broadly defined the field of endeavor for the ’376 Patent as a “system or method in which a user interacts with ‘a first [electronic] device and a second [electronic] device throughout the use of an online application.”” PG at 18, 24-25. In response, Dr. Rubin has modified the claims to specify all the Substitute Claims are explicitly directed toward enhancing information security. The Board should modify its field of endeavor to “system or method to protect information where a user interacts with ‘a first [electronic] device and a second [electronic] device throughout the use of an online application.””

The Federal Circuit’s decision in *Airbus S.A.S. v. Firepass Corporation* is instructive. *See* 941 F.3d 1374, 1379-81 (Fed. Cir. 2019). Airbus argued an “air system” used for a gyms was analogous prior art to an “air system” used for fire prevention and suppression. *Airbus*, 941 F.3d at 1381-82. The court noted that “[t]o determine the applicable field of endeavor, the factfinder must consider ‘explanations of the invention’s subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.’” *Id.* at 1380. The court considered the written description and the claims including the title of the

Patent, embodiments in the specification and the preamble of the claims. In each instance, the subject matter was clearly air systems for fire prevention.

Here, the facts are even stronger for construing Dr. Rubin's patent in the field of security. The preamble and the claims both specify the invention is directed towards enhancing security. The abstract, the introduction and the field of invention all make clear that the field of endeavor is protecting information with two devices during the use of an online application. Ex. 2005, ¶¶2, 18, 58.

Neither *Zha*, *Takahashi* nor *Tsushima* are within the '376 Patent's field of endeavor as all three have nothing to do with security.³ Similarly, all three references seek to solve a different problem. *Zha* seeks to reduce network traffic by reducing unnecessary data sent to multiple devices. *Takahashi* offers an improved game controller for social games, and *Tsushima* offers an improved controller for watching streaming video or playing games on two devices. Ex. 2008, ¶¶188-92. All three references are not analogous art.

VI. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests the Board grant this motion and substitute claims 26-41 as set forth in Appendix A.

³ The Patent Owner concedes that *Kling* and *Lipetz* are good examples of prior art references within the same field of endeavor as the '376 Patent.

Dated: April 5, 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@vbllaw.com
Counsel for Patent Owner

APPENDIX A

LISTING OF CLAIMS

Patent Owner presents the following non-contingent substitute claims.

Pursuant to 37 C.F.R. § 1.121(c)(2), the use of strikethroughs/brackets indicate deleted text and underlining indicates inserted text. Bolded text indicates changes made to the Substitute Claims in the Revised Motion only.

Listing of Claims:

Claims 1-5 (canceled)

6. (not challenged) The method of claim 5, further comprising determining by an absence of a heartbeat if the connectivity has been disrupted and receiving an election from the user whether or not to switch to using only the first device for subsequent communications.

7. (not challenged) The method of claim 1, further comprising:
detecting whether the second device has received the second subset of the information;

displaying the second subset of the information on the second device; and
generating an indicator on the first device indicating that the second device has received the second subset of the information.

8. (not challenged) The method of claim 7, wherein if the first device has not received the indication that the second device has received the second subset of the information, then a user's turn in an online game is delayed.

Claims 9-10. (canceled)

11. (not challenged) The method of claim 10, wherein 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.

Claims 12-17. (canceled)

18. (not challenged) The method of claim 17, wherein the first device provides a visual mark on each of multiple tables that is displayed that matches a visual mark on the hole cards that are displayed on the second device to keep the hole cards and the tables synchronized.

19. (not challenged) The method of claim 17, wherein the game server provides information to identify the table to which table the hole cards belong.

20. (not challenged) The method of claim 17, wherein the first device communicates to the game server which table has focus, and wherein the game server then communicates to the second device an instruction to display the hole cards that correspond to an active table that has the focus in the first device.

21. (not challenged) The method of claim 17, wherein a user is playing more than one poker table, and wherein the first device communicates to the second

device information indicating which hole cards to view on the second device corresponding to an active table having focus on the first device.

22. (not challenged) The method of claim 1, wherein the set of information at a server represents financial record information and the first subset of the information comprises account identifying information and the second subset of the information comprises account balance information.

Claims 23-25. (cancelled)

[[1.]] 26. (Substitute for Claim 1) A method for **protecting information by** transmitting information to multiple electronic devices, the method comprising:

electronically storing a set of information at a server;

identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;

determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information **that is not authentication information specific to a device** at both the first and second devices, wherein the

application specific authentication information used on the first device is different from the application specific authentication information used on the second device;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting [[a]] the first subset of the information to the first device from the server; and

transmitting [[a]] the second subset of the information to the second device from the server,

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.**

[[2.]] 27. (Substitute to Claim 2) The method of claim [[1]] 26, further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.

[[3.]] 28. (Substitute for Claim 3) The method of claim [[1]] 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information **and the sensitive information is only shared with the second device.**

[[4.]] 29. (Substitute for Claim 4) The method of claim [[1]] 26, wherein the information received at the second device is more sensitive than the information received at the first device.

[[5.]] 30. (Substitute for Claim 5) The method of claim [[1]] 28, further comprising:

determining if connectivity between the server and the second device has been disrupted; and

providing a notification **by the application** on the second device that the connectivity has been disrupted.

[[9.]] 31. (Substitute for Claim 9) The method of claim [[1]] 26, wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.

[[10.]] 32. (Substitute for Claim 10) The method of claim [[1]] 26, further comprising 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.

[[12.]] 33. (Substitute for Claim 12) The method of claim [[1]] 26, wherein the information received at the second device is a user's private cards in an online card game.

[[13.]] 34. (Substitute for Claim 13) The method of claim [[1]] 26, wherein the a display on the first device is being viewed exclusively by a first user and a display on a second device is also being viewed exclusively by the first user.

[[14.]] 35. (Substitute for Claim 14) The method of claim [[1]] 30, wherein, neither the first subset of information nor the second subset comprise a two factor authentication code, and,

further comprising 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.

[[15.]] 36. (Substitute for Claim 15) The method of claim [[1]] 26, wherein the server is a proxy server configured to relay communications from an application server to the first and second devices wherein the proxy server emulates a client to the application server.

[[16]] 37. (Substitute for Claim 16) The method of claim [[1]] 26, further comprising configuring the server for managing an online game, and wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, wherein the first electronic device is primarily used to play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.

[[17.]] 38. (Substitute for Claim 17) The method of claim [[16]] 37, wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.

[[23.]] 39. (Substitute for Claim 23) he method of claim [[1]] 26, further comprising electronically storing at the server a parameter indicating whether subsets of the information are to be divided between two or more devices.

[[24.]] 40. (Substitute for Claim 24) The method of claim [[1]] 26, wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.

[[25.]] 41. (Substitute for Claim 25) A system for **protecting information** **by** transmitting information to multiple electronic devices, the system comprising:

an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;

a processor device programmed for:

identifying a first subset of the information and identifying a second subset of the information;

determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and

being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information **that is not authentication information specific to a device** at both the first and second devices;

wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device;

if and only if both the first and second devices are determined to be accessible by the server, then:

transmitting [[a]] the first subset of the information to the first device from the server; and

transmitting [[a]] the second subset of the information to the second device from the server,

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.**

CERTIFICATE OF FILING AND SERVICE

I hereby certify that a true and correct copy of the foregoing PATENT OWNER'S REVISED MOTION TO AMEND is being filed electronically via PTAB E2E and served on counsel for Petitioner by electronic mail this 5th day of April, 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: April 5, 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