

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
REVISED 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

May 22, 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)
1029	Third Declaration of Sigurd Meldal, Dr. Scient
1030	U.S. Patent Pub. No. 2013/0023241 (“ <i>Lim</i> ”)
1031	U.S. Patent No. 7,676,829 (“ <i>Gui</i> ”)
1032	Deposition Transcript of Patrick Traynor – May 13, 2024 (condensed)

TABLE OF CONTENTS

I.	INTRODUCTORY STATEMENT	1
II.	CLAIMS 26 AND 41 LACK WRITTEN DESCRIPTION SUPPORT.....	1
III.	CLAIM 28 LACKS WRITTEN DESCRIPTION SUPPORT	1
IV.	CLAIMS 32 AND 35 ARE INDEFINITE.....	2
V.	NEW “THEREBY” CLAUSE DOES NOT LIMIT THE CLAIMS	3
VI.	<i>ZHA</i> GROUNDS.....	4
A.	CLAIM 26 (GROUNDS 1-2)	4
B.	CLAIM 27 (GROUNDS 1-2)	7
C.	CLAIM 28 (GROUNDS 1-2)	8
D.	CLAIM 29 (GROUNDS 1-2)	8
E.	CLAIM 30 (GROUNDS 3-4)	8
F.	CLAIM 31 (GROUNDS 1-2)	8
G.	CLAIM 32 (GROUNDS 5-6)	9
H.	CLAIM 34 (GROUNDS 1-2)	9
I.	CLAIM 35 (GROUNDS 7-8)	9
J.	CLAIM 37 (GROUNDS 1-2)	10
K.	CLAIMS 39, 40 (GROUNDS 1-2).....	11
L.	CLAIM 41 (GROUNDS 1-2)	12
VII.	<i>ZHA</i> GROUNDS 1-8 COMBINED WITH <i>GUI</i>	13
VIII.	RESPONSE TO PO’S ARGUMENTS RE: <i>ZHA</i> GROUNDS.....	15
IX.	<i>KLING</i> GROUND: CLAIMS 26–29, 31–32, 34–35, AND 39–41 ARE OBVIOUS OVER <i>KLING</i> , <i>LIM</i> , AND A POSITA’S KNOWLEDGE.....	17
A.	OVERVIEW: <i>KLING</i>	17
B.	INDEPENDENT SUBSTITUTE CLAIM 26	17
C.	DEPENDENT SUBSTITUTE CLAIMS	27
D.	INDEPENDENT SUBSTITUTE CLAIM 41	31

X. <i>TAKAHASHI</i> GROUNDS	32
XI. RESPONSE TO PO’S ARGUMENTS RE: <i>TAKAHASHI</i> GROUNDS	33
XII. <i>TAKAHASHI</i> GROUNDS COMBINED WITH <i>GUI</i>	34

TABLE OF AUTHORITIES

CASES

<i>Lockheed Martin Corp. v. Space Sys./Loral, Inc.</i> , 324 F.3d 1308 (Fed. Cir. 2003)	3
<i>Nautilus, Inc. v. Biosig Instruments, Inc.</i> , 572 U.S. 898 (2014)	2
<i>Texas Inst. Inc. v. U.S. Int’l Trade Comm’n</i> , 988 F.2d 1165 (Fed. Cir. 1993)	3

I. INTRODUCTORY STATEMENT

The Board should deny PO's Revised Motion to Amend ("RMTA").

II. CLAIMS 26 AND 41 LACK WRITTEN DESCRIPTION SUPPORT

Substitute claims 26 and 41 recite that the application specific authentication information is "not authentication information specific to a device at **both** the first and second devices" (emphasis added). That is, the application specific authentication information cannot be device specific for **either** the first or the second device. Ex-1029, ¶4. Patent Owner cites Fig. 10, ¶26, ¶33, ¶75, ¶83, ¶89, ¶90, ¶92 of the '995 Application as support for this new feature. RMTA at 3; Ex. 2008 at ¶68. At best, these portions disclose that the application specific authentication information for the second device is not device specific. Ex-1029, ¶4. For example, paragraph 92 discloses that the authentication information (such as a password) should allow for authentication on any **second** device. Ex. 2005 at ¶92. **But that disclosure relates only to the second device, and a POSITA would not read that as similarly applicable to the authentication information for the first device.** Ex-1029, ¶4. Thus, there is insufficient written description support for claims 26 and 41, and all substitute claims that depend therefrom.

III. CLAIM 28 LACKS WRITTEN DESCRIPTION SUPPORT

PO's arguments attempting to distinguish the prior art (*Zha*) based on "sensitive information is only shared with the second device" (RMTA, 17; Ex-2008 ¶112) suggest that PO understands limitation [28b] to mean that sensitive

information cannot have been transmitted, shared, communicated, or disclosed to any other device, at any time. Ex-1029, ¶¶6-9. If this is what the new term means, there is no written description support because nothing in the specification teaches that the sensitive information that is transmitted to the second device cannot ever be shared, disclosed, or communicated to any other device or person. Ex-1029, ¶¶10-11. In fact, the '376 Patent expressly discloses communicating the sensitive information with the first device and other users, for example, sensitive hole cards sent to the second device are communicated to the first device and all other players in the poker game embodiment. Ex-1029, ¶¶11-12 (*citing, e.g.,* Ex-1001, 5:56-63).

IV. CLAIMS 32 AND 35 ARE INDEFINITE

The phrase “the information displayed on the respective devices,” recited in claims 32 and 35 is indefinite under § 112(a) because its scope cannot be determined with reasonable certainty. *See Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). First, the phrase lacks antecedent basis. Second, the phrase is ambiguous because it is unclear whether “the information” refers to one or more of the types of “information” in claim 26, i.e., “a set of information at a server” (element [26a]), “a first subset of the information” (element [26b]), “a second subset of the information” (element [26b]), “application specific authentication information” (element [26c]), and “information not transmitted to the first device” (element [26d]). RMTA at 3-4. While one of these could be “the information” to which claims

32 and 35 refer, none of the claims recite displaying that information, casting further doubt on the meaning of “the information *displayed* on the respective devices.” Alternatively, “the information” could refer to the “graphical identifier” and the “corresponding graphical indicator” in claims 32 and 35 which are “display[ed]” on the first device and the second device. Neither the specification nor the file history clarify the ambiguity. Ex-1029, ¶¶15-19.

V. NEW “THEREBY” CLAUSE DOES NOT LIMIT THE CLAIMS

The clause—“thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device”—in revised substitute claims 26 and 41, merely states a result and does not constitute a limitation entitled to patentable weight. Ex-1029, ¶¶25-30. *See Texas Inst. Inc. v. U.S. Int’l Trade Comm’n*, 988 F.2d 1165, 1172 (Fed. Cir. 1993) (concluding, in process claims, that the whereby clauses described “the result of arranging the components of the claims in the manner recited in the claims” and thus were not limitations); *Lockheed Martin Corp. v. Space Sys./Loral, Inc.*, 324 F.3d 1308, 1319 (Fed. Cir. 2003) (same). Limitations [26d] and [41e] recite that “the second subset of the information includes information not transmitted to the first device.” Thus, the second subset of information would not be susceptible to compromise by malware on the first device because it isn’t transmitted to the first device. Ex-1029, ¶¶27-28. PO’s expert appears to agree. Ex-1032, Traynor Dep. Tr. Vol. II, 186:11-20, 184:18-

186:20 (“Malware cannot access or compromise the information that it cannot see.”). The implication of this is that if a prior art discloses “the second subset of the information includes information not transmitted to the first device,” it necessarily discloses the claimed result associated with malware protection.

VI. ZHA GROUNDS

Claims 26-32, 34, 35, 37, and 39-41 are obvious in view of *Zha*, other prior art cited in the Petition (“Paper 2”), and the POSITA’s general knowledge (“PGK”). Ex-1029, ¶¶192–236. The *Zha* Grounds are all based on § 103 and include: (Ground 1) *Zha*+PGK, claims 26-29, 31, 34, 37, 39-41; (Ground 2) *Zha*+PGK+*Tsushima*, claims 26-29, 31, 34, 37, 39-41; (Ground 3) *Zha*+PGK+*Gumbula*, claim 30; (Ground 4) *Zha*+PGK+*Tsushima*+*Gumbula*, claim 30; (Ground 5) *Zha*+PGK+*Stafford*, claim 32; (Ground 6) *Zha*+PGK+*Tsushima*+*Stafford*, claim 32; (Ground 7) *Zha*+PGK+*Stafford*+*Gumbula*, claim 35; (Ground 8) *Zha*+PGK+*Tsushima*+*Stafford*+*Gumbula*, claim 35.

A. Claim 26 (Grounds 1-2)

Claim 26 is rendered obvious by *Zha* and POSITA’s knowledge. Ex-1002 ¶¶57-92; Ex-1029, ¶¶192–236. [26Pre]¹: *Zha* discloses a method for sending data

¹ [26pre], [26a], and so forth refer to the claim limitations of the revised substitute claims as set forth on pages 3-7 of the RMTA.

to first and second terminals, with reference to Figure 2B. Ex-1004, 5:10-38. Ex-1002 ¶¶57-58; Ex-1029, ¶¶192-236; *see also* Paper 2, 8. **[26a]:** *Zha*'s functional interface data is "a set of information" electronically stored at server 120. Ex-1004, 4:22-24, 4:36-44, 5:35-37, 22:45-46, 29:11-17, Figure 2; Ex-1002 ¶¶59-60; Ex-1029, ¶¶192-236; *see also* Paper 2 at 8-9. **[26b]:** *Zha*'s private message interface data corresponds to the "second subset of information," and other functional interface data (homepage and game interface data) corresponds to the "first subset of information." Ex-1004, 18:66-19:13, 5:22-27, Figure 2B. Ex-1002 ¶¶63-70; Ex-1029, ¶¶192-236; *see also* Paper 2 at 9-10. *Zha*'s microblog application corresponds to the "same application." Ex-1004, 7:33-44, 17:48-53, 18:11-17, 19:3-13; *see also* Ex-1004, Abstract ("determining a first terminal and a second terminal currently *using the same application* with the same account;"). *Zha*'s functional interface data is "specific to that application" because the interfaces are associated with the microblog application. Ex-1002 ¶68. *Zha* discloses the application at the server generates the functional interface data. Ex-1004, 18:66-19:13. Ex-1002 ¶69; Ex-1029, ¶¶192-236; *see also* Paper 2 at 10-11.

[26c]: *Zha* discloses a login process to determine whether a single user has logged into the same microblog application at two terminals. Ex-1004, 5:19-21, 18:41-49; Ex-1002 ¶75; Ex-1029, ¶¶192-236; *see also* Paper 2 at 11-12. 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-1029, ¶¶196–97. Evidence that a POSITA knew a user could use different authentication information (i.e., different passwords) to login to the *Zha* microblog application at two terminals is found in U.S. Patent No. 7,676,829 (“*Gui*”), U.S. Patent No. 7,865,950 (“*Lipetz*”), and *Kling*. Ex-1029, ¶¶196–204. *Gui*, *Lipetz*, and *Kling* relate to securing computer systems against malware (Ex. 1031, 2:55-61; Ex. 1025, 1:6-7, 1:63-66; Ex. 1023, [0005][0015]) and motivate a POSITA to use different passwords with *Zha*’s microblog application to enhance security against malware in a computing system using multiple devices. Ex-1029, ¶¶205-11. Furthermore, the passwords are not device specific because *Zha* does not disclose that the logins from the two terminals are specific to those two terminals. Ex-1029, ¶196. *Zha*’s terminals communicate with the server over a wired or wireless network, i.e., are “accessible over at least one electronic communications network.” Ex-1004, 4:22-29. Ex-1002 ¶79; *see also* Paper 2 at 11-12.

[26d]: *Zha* discloses the “if and only if” claim element because (1) *Zha*’s server transmits distinct data to both terminals when the server determines both terminals are accessible by the server (i.e., after the user has logged in with both terminals); and (2) *Zha*’s server does not transmit distinct data to both terminals when the server determines both terminals are not accessible by the server. Ex-1002 ¶¶85-86; *see also* Paper 2 at 13-15. *Zha*’s server sends private message interface data

(“second subset of information”) to a cellphone (“second device”) and other functional interface data, such as for the homepage and game interfaces, (“first subset of information”) to a desktop computer (“first device”). Ex-1004, 18:66-19:13. Ex-1002 ¶¶81; *see also* Paper 2 at 13-15. *Zha*’s server sends a “private message only to the cellphone” but sends other non-private message data to the desktop computer. Ex-1004, 18:63-19:13. That is, *Zha*’s “second subset of the information includes information not transmitted to the first device.” Ex-1004, 19:13-19, 5:22-27, Figure 2B (S203, S205), 18:66-19:13. Ex-1002 ¶¶82-84. Further, a POSITA knew to transmit information “if and only if” the user has logged into the *Zha* microblog application at two terminals. Ex. 1030 ¶[0077]; Ex-1029, ¶¶128-39. For example, *Tsushima* (Ex. 1010) discloses “[i]n step S503, the server CPU 201 determines *whether or not login to a service succeeded on both* an operation input device (the portable terminal 100) and a screen display device (the PC 300) for a user ID that is a target of service provision.” Ex. 1010, [0059] (emphasis added), Figure 5 (S503), [0061].

B. Claim 27 (Grounds 1-2)

As discussed above for claim 26, *Zha*’s server transmits the main interface data (at least a “portion” of the first subset) to the cellphone and then transmits the private message interface data to the cellphone. Ex-1002 ¶¶93-96; *see also* Paper 2 at 15-16. This transmission happens “if and only if” both logins are successful. *See*

analysis above for [26d].

C. Claim 28 (Grounds 1-2)

Zha's server "only shares" the sensitive private message (sensitive) to the cellphone terminal ("second device") and sends the homepage (non-sensitive) information to the desktop computer ("first device"). Ex-1004, 18:63-19:13. Ex-1002 ¶¶99-100; Ex-1029, ¶¶212-214; *see also* Paper 2 at 16-17.

D. Claim 29 (Grounds 1-2)

The private message to the cellphone ("second device,") are more sensitive compared to the homepage information. Ex-1004, 16:62-17:1, 18:66-19:13; Ex-1002 ¶101; *see also* Paper 2 at 17.

E. Claim 30 (Grounds 3-4)

Claim 30 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 claim 28 (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-1011, Abstract, 1:56-60, 4:44-49; Ex-1029, ¶¶217–18; *see also* Paper 2 at 16-17.

F. Claim 31 (Grounds 1-2)

At least two terminals and a server are connected via "a *wired network or a wireless network*," which are independent. Ex-1004, 4:27-29, Figure 1. Ex-1002

¶¶102-103; *see also* Paper 2 at 17-18. *Wakeford* (Ex-1013) is evidence a POSITA knew client-server applications (such as *Zha*) are capable of transmitting “over independent electronic communications networks.” Ex-1002 ¶¶104-105; *see also* Paper 2 at 18-19.

G. Claim 32 (Grounds 5-6)

Claim 32 recites the “graphical identifier” limitation, wherein PO did not dispute that *Stafford* is properly combined with *Zha* in Grounds 5–6 (cl. 10) or that *Stafford* discloses the same limitation now recited in claim 32. Ex-1012, [0008][0030][0064][0065], Figure 7; Ex-1029, ¶¶221–22; *see also* Paper 2 at 32-47.

H. Claim 34 (Grounds 1-2)

A POSITA understood the private message interface would be viewed exclusively by the single user for whom the private messages were intended. Ex-1002 ¶¶106-107; Ex-1029, ¶¶163-165 (*Lim* user terminal 50 and mobile terminal 100 are viewed exclusively by user. Ex. 1030, [0028]); *see also* Paper 2 at 19.

I. Claim 35 (Grounds 7-8)

Zha makes no reference to employing two factor authentication codes. Ex-1002 ¶108; *see also* Paper 2 at 19.

This claim depends from claim 30, claim 28, and claim 26, and adds the “graphical identifier” limitation from claim 32. Claim 35 is obvious based on *Zha*, a POSITA’s general knowledge, *Gumbula*, and *Stafford* (Ground 3 combined with Ground 5 and the POSITA’s general knowledge of multiple/different passwords as

disclosed in *Gui*, *Lipetz*, and *Kling*) or, alternatively, by *Zha*, a POSITA's general knowledge, *Tsushima*, *Gumbula*, and *Stafford* (Ground 4 combined with Ground 6 and the POSITA's general knowledge of multiple/different passwords as disclosed in *Gui*, *Lipetz*, and *Kling*). 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-1029, ¶¶216–18; *see also* Paper 2 at 32-47.

J. Claim 37 (Grounds 1-2)

“[M]icroblog may provide a homepage functional interface, a private message functional interface and a *game functional interface*.” Ex-1004, 7:32-44, Figure 1. *Zha* discloses a server managing an “*online*” game because the terminals are

connected to the server over a network. Ex-1004, 4:27-29. Ex-1002 ¶110; *see also* Paper 2 at 20. *Zha*'s server 120 communicates with "[a]t least two terminals 110, which run an application program with the same account simultaneously." Ex-1004, 4:22-29, 4:36-44, Figure 1; Ex-1002 ¶¶110-112; *see also* Paper 2 at 20. The *Zha* desktop computer is the "first electronic device [and] is primarily used to play the game" where "the server may assign an access permission for accessing the game interface to the desktop computer." Ex-1004, 7:42-44; Ex-1002 ¶113; *see also* Paper 2 at 20. *Zha*'s server only sends the private message ("sensitive information") to the cellphone ("second device") and not to the desktop computer ("first device.") Ex-1004, 18:66-19:13; Ex-1002 ¶¶114-115; *see also* Paper 2 at 21.

K. Claims 39, 40 (Grounds 1-2)

Claim 39: The *Zha* access permission corresponds to the "parameter." "[D]ata corresponding to each of the functional interfaces is only assigned to a terminal having an access permission for accessing the functional interface..." Ex-1004, 5:48-53, 5:22-27, Figure 2B; Ex-1002 ¶¶116-117. Because the access permissions are distinct for each terminal, the access permissions correspond to a "parameter" indicating whether subsets of information are to be divided between two or more terminals. Ex-1002 ¶118; *see also* Paper 2 at 22-24.

Claim 40: The *Zha* homepage, private messaging, and game functional interface data are each "application specific" "subsets of information" that "derive

from functions within” the microblog. Ex-1004, 7:33-44, 17:48-53, 18:11-17, 19:3-13; Ex-1002 ¶¶119-121; *see also* Paper 2 at 24.

L. Claim 41 (Grounds 1-2)

[41Pre]: A server (“system”) sends data to a first terminal and a second terminal (“multiple electronic devices”). Ex-1004, 4:22-24, 22:16-33, Figure 1. Ex-1002 ¶¶122-123; *see also* Paper 2 at 24. **[41a]:** “[T]he server may be in the form of software, hardware or a combination of both” (Ex-1004, 22:45-47), which corresponds to the “electronic data store” for “electronically storing a set of information at the server.” Ex-1004, 4:36-46, 29:11-17. Ex-1002 ¶¶124-125; *see also* Paper 2 at 24-25. **[41b]:** Notably, “the first and second subsets of information” lacks antecedent basis. If this phrase refers to “a first subset of the information” and “a second subset of the information” that appear later in the claim, *Zha* discloses this because the same limitation is found in claim 26 and a similar limitation is found in claim 40. *Zha* discloses this element as explained for claim elements [26b] and [40a]. Ex-1002 ¶¶126-127; *see also* Paper 2 at 25. **[41c]:** *Zha*’s server is a combination of hardware and software for running an application program (Ex-1004, 17:44-46, 22:45-47), such as microblog (Ex-1004, 1:25). *Zha*’s server corresponds to the “processor device programed for.” A server necessarily includes a processor programmed to perform the server’s functions. *See* Ex-1007, [0062] (a processor (CPU) is part of the game server); Ex-1002 ¶¶128-129; *see also* Paper 2 at 25-26.

[41d]: *Zha* discloses this element as explained for claim element [26c]. Ex-1002 ¶130; *see also* Paper 2 at 26. [41e]: *Zha* discloses this element as explained for claim element [26d]. Ex-1002 ¶131; *see also* Paper 2 at 26.

VII. ZHA GROUNDS 1-8 COMBINED WITH GUI

If PO argues for Grounds 1-8 that a POSITA's knowledge does not render obvious limitation [26c] because, for example, PO contends that a POSITA lacks knowledge of a user accessing an account using multiple passwords on multiple devices, [26c] would have obvious in further view of *Gui*. *Gui* is prior art under 35 U.S.C. § 102(a) because it was filed in 2001 and issued in 2010. *Gui*, which is directed to “systems and methods for associating multiple credentials with a single user account” discloses utilizing different credentials (e.g., a password/username combination) to access the same application from different devices. Ex. 1031, Abstract, 9:11-17, 6:27-31, 6:65-7:6, 2:55-61, 2:20-29. *Gui*'s multiple credentials constitute “application specific authentication information.” And the credentials are not “device specific” because a credential can be used on the same category of devices (e.g., different cellular phones) or even on “any device.” *Id.*, 10:21-33.

It would have been obvious to combine *Gui*'s use of multiple/different passwords for different devices with *Zha*'s microblog application such that *Zha*'s microblog application allows different passwords to access the same user account from the two terminals. Ex-1029, ¶¶237–245. A POSITA would have been

motivated to combine the teachings because “a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device” (Ex-1031, 2:24-29). Ex-1029, ¶¶243-45.

The use of different application specific authentication information (e.g., passwords) for accessing *Zha*’s microblog from a mobile phone versus from a desktop/laptop computer is merely an example of combining prior art elements (multiple passwords in place of a single password) according to known methods to yield predictable results (allowing the same user to access a service/account from different devices). A POSITA would also find this modification to be the simple substitution of one known element (multiple password system) for another (single password system) to obtain predictable results (allowing the same user to access a service/account from different devices). Further, using multiple passwords for different devices is a predictable use of prior art elements (*Gui*’s multiple passwords) according to their established functions (allowing one user to access the same application/account with different passwords on different devices). Finally, this combination merely applies a known technique (multiple passwords for accessing the same application/account) to a known device (*Zha*’s online microblog) ready for improvement (to make it easier for users logging on with limited human interface options such as a cell phone) to yield predictable results (successful login to the same account with different passwords). Ex-1029, ¶244.

Given the disclosure in *Gui* and a POSITA's knowledge of how to implement relevant software functionality, a POSITA would have a reasonable expectation of success of combining *Gui* and *Zha*. Indeed, *Zha* does not go into details regarding the exact implementation of its login authentication because, by 2014, that was a trivial function of an application. This is also why the disclosures of *Gui*, *Lipetz*, and *Kling* of different passwords in an application are high-level (and without much implementation detail)—implementing a password authentication mechanism, including multiple passwords, in an application was well within the POSITA's knowledge before 2014. Ex-1029, ¶ 245.

VIII. RESPONSE TO PO'S ARGUMENTS RE: ZHA GROUNDS

“Authentication Information”: PO's argument that *Zha* does not mention “authentication information” that is different for two devices (RMTA at 13) 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-1029, ¶223. It is undisputed that password authentication for an application like *Zha*'s microblog (e.g., Facebook) is “application specific.” Ex-1029, ¶223; Ex-1026, 72:4–9 (“My username and password that I use for social media application, that's specific to that application.”).

Using different passwords for the different devices was well known, as evidenced by at least *Gui*, *Lipetz*, and *Kling*. Ex-1029, ¶¶223-30. *Gui* provides

motivation to use different authentication information based on the accessibility of the different human interfaces of the *Zha* laptop computer, cellphone, and desktop computer. Ex-1029, ¶224. *Zha*'s disclosure of logging into the microblog, in view of the POSITA's knowledge shown by *Gui*, *Lipetz*, and *Kling*, renders obvious using different application specific authentication information for determining login to the application at the first and second devices. Ex-1029, ¶230.

Preamble and “thereby” limitation ([26d] & [41d]): PO's argument that *Zha* does not meet the preamble and “thereby” limitations (RMTA at 16) should be rejected because neither the preamble nor the “thereby” clause further limit the claim. See Section III; Ex-1029, ¶231. Regardless, a POSITA understands that *Zha* protects information because information that is not transmitted to a device is protected from malware on that device. Thus, if a user configures *Zha* to send private messages only to the user's phone, that information will be protected from malware on the user's desktop computer while that setting remains.

“sensitive information is only shared with the second device”: PO's argument that *Zha* does not disclose this limitation because private messages are shared beyond the second device (RMTA, 17) contradicts every embodiment disclosed in the '376 Patent: hole cards (poker embodiment) are shared with every player in the game, bank transaction information (banking embodiment) is shared with bank employees and recipients of funds transfers, and health information (health care

portal embodiment) is shared with medical providers. Given its plain meaning in the context of the claim, *Zha*'s private messages, in the two-device embodiment where *Zha* is configured to send private messages to the user's cell phone, renders this claim obvious. Ex-1029, ¶¶232-36. PO's additional argument that *Zha* is distinguishable because the private chat app is accessible on the first device (RMTA, 17) is a red herring that focuses on *Zha*'s single-device embodiment, whereas Petitioner relies on *Zha*'s two-device embodiment where information is only shared with the second device. Ex-1029, ¶¶232-36.

IX. KLING GROUND: CLAIMS 26–29, 31–32, 34–35, AND 39–41 ARE OBVIOUS OVER KLING, LIM, AND A POSITA'S KNOWLEDGE

A. Overview: *Kling*

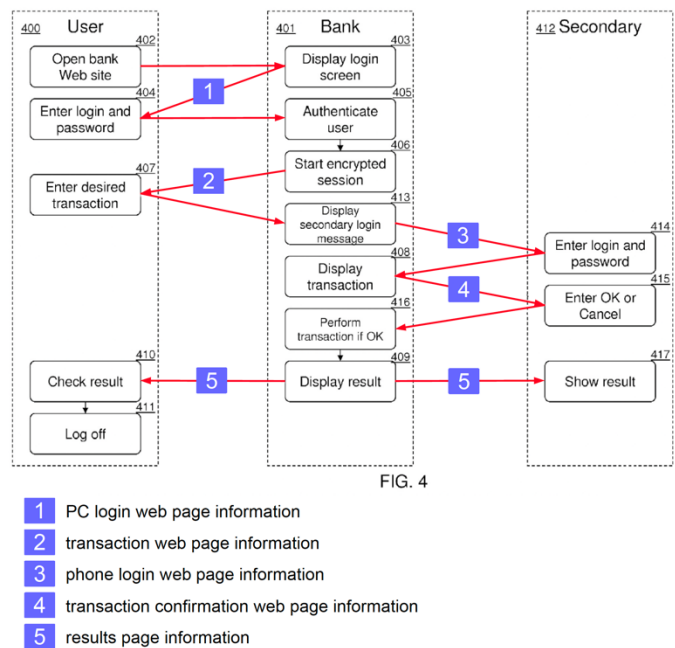
U.S. Patent Pub. No. 2012/0240203 (“*Kling*”) (Ex-1023) is prior art under 35 U.S.C. § 102(a) because it published September 20, 2012. Ex-1023, [22][43]. *Kling* is directed to enhancing online security for a user transacting with a server using a first device (e.g., a PC) by obtaining secondary confirmation from the user on a second device (e.g., a phone). Ex-1023, [57], ¶[0013]; Ex-1029, ¶¶46–47. 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-1029, ¶¶119–120.

B. Independent Substitute Claim 26

[26Preamble]: *Kling* discloses this element. Ex-1029, ¶¶70–74. *Kling* discloses a bank server 401 transmitting information to a user's PC and a user's

mobile device. Ex-1023, Figure 4, ¶¶ [0017]-[0018]. **[26a]:** *Kling* discloses this element. Ex-1029, ¶¶75–81. *Kling* discloses “[a] flow chart of the user’s transactions 200 with a remote server 201 are shown in FIG. 2. Typically, the user would open a Web site 202, in this example of a bank.” Ex-1023, ¶ [0014]. The *Kling* web site 202 corresponds to the claimed “electronically storing a set of information at a server.” Ex-1029, ¶75. A POSITA understands a website includes web page information that provides a set of sufficiently specific web page information to allow the user to enter the specific transaction the user desires to engage in. Ex-1029, ¶76. A POSITA understands that servers such as *Kling*’s bank server are capable of storing information because it was well-known in the art that servers stored information that they were tasked with providing to client devices. Ex-1029, ¶77.

[26b]: *Kling* discloses this element. Ex-1029, ¶¶82–87. *Kling* identifies distinct subsets of information specific to “the Web site 202, in this example of a bank.” Ex-1023, ¶[0014]. Figure 4 is annotated to identify information being transmitted. Ex-1023, Figure 4



(annotated)²; Ex-1029, ¶¶83-85. First, the transaction web page information [Arrow #2] sent to the user's PC for the user to "enter desired transaction 407" corresponds to the claimed "first subset of information." Second, the transaction confirmation web page information [Arrow #4] sent to the mobile device to display the transaction 408 and for the user to "enter OK or cancel" 415 corresponds to the claimed "second subset of information." Both web pages for the PC "session" and the mobile device "session" are generated by server banking application (Web site 202) at the server 401 and are specific to the banking application. Ex-1029, ¶84.

[26c]: *Kling* teaches this limitation by disclosing the bank server determining if the user's PC and mobile phone are accessible by requiring a user to separately log into the banking application via both devices using different passwords. Ex-1029, ¶¶88-127; Ex-1023, ¶¶[0014], [0017]-[0019] & Figs. 4-5.

PO is incorrect that *Kling*'s login by the mobile device uses device-specific authentication information. *See* RMTA at 9-10. As a "comprising" claim, element [26c] does not preclude use of device specific information for other purposes in the system (e.g., used *by the server* to determine the availability of a user's secondary device). Ex-1029, ¶¶99-100. Further, a POSITA understands that even though *Kling*

² Subsequent citations to "Arrow #X" for the *Kling* reference refer to the arrows in this annotated figure.

uses the language “log into the mobile device,” this means that the user would be prompted to log into the bank server on the mobile device. Ex-1029, ¶¶101-105. A POSITA understands this because element/step 413 “display secondary login message” is described as the bank server “invok[ing] a secondary authentication request 413” (Ex-1023, ¶ [0017]) and sending a login page to the mobile device (Figure 4). If, as PO suggests, the user were simply logging into the mobile device and not the bank server, there would be no need for the bank server to invoke a secondary authentication request or display a secondary login message on the mobile device. There would also be no reason for the user to “[e]nter login and password” (414) in response to the bank server’s transmitting the “[d]isplay secondary login message.” For these reasons, a POSITA understands that *Kling*’s system requires the user of the mobile device to login to the bank server, i.e., “ideally using a different password than on the PC.” Ex-1023, ¶ [0017]. Ex-1029, ¶¶101-105. Further, both passwords are not device specific as there is nothing in *Kling* remotely suggesting that either password can only be used at a specific device.

Even assuming *arguendo* that *Kling* teaches device specific authentication information, *Lim* teaches element [26c]. Ex-1029, ¶¶106-127. *Lim* (Ex-1030) is prior art under at least 35 U.S.C. § 102(a)(2) because it was effectively filed on September 26, 2012, and published on January 24, 2013. Ex-1023, [22][43]. *Lim* is directed to authentication using a user terminal, such as a PC, and a portable terminal, such as

a mobile phone. Ex-1030, ¶ [0054]. In *Lim*, a user on terminal 50 first authenticates himself to a service server 300 through, for example, an identifier/password. *Id.*, ¶¶[0028], [0029]. Mobile terminal 100 captures an image of identifier 60 displayed on user terminal 50, and sends the identifier 60 to authentication system 200. *Id.*, ¶[0033]. If the authentication system 200 determines that the identifier 60 is valid (*id.*, ¶[0038]), system 200 requests authentication information from mobile terminal 100. (*Id.*) The user of the mobile terminal 100 then authenticates with system 200 by providing an identifier/password, a user-specific authentication number, or a user's biometric information (e.g., iris, fingerprint, or voice) “thereby performing a final authentication process.” (*Id.*, [0038]-[0041]); Ex-1029, ¶¶63-66. If the authentication is successful, authentication system 200 “notifies the service server 300 of the success of the authentication.” (Ex-1030, ¶¶[0067], [0076].)

Once the success of the authentication has been notified . . . the service server 300 determines that the user terminal 50 has been successful in the authentication, allows normal access, and provides a variety of services that can be utilized by a login user. If the service server 300 is the server of a financial institution, such as a bank, the service server 300 allows the user terminal 50 to do an account transfer, search an account, use a loan service, pay a utility bill, and use a variety of services that are provided by the financial institution such as a bank.

Ex-1030, ¶ [0077].

Lim thus discloses a user using two different authentication mechanisms (two different “application specific authentication information”) from two different devices to access an application. The authentication number and biometric information used for authentication on the second device (mobile terminal) are different from the identifier/password on the first device (terminal 50). While *Lim* is silent as to whether the identifier/password used to authenticate the first device is the same or different from the identifier/password used to authenticate the second device, a POSITA knows based on *Kling* that they “ideally” should be different. *Id.* (citing Ex-1023, ¶[0017]). A POSITA further knows these types of authentication information are not device specific. Ex-1029, ¶¶112-116.

It would have been obvious to modify *Kling* as taught by *Lim*. Ex-1029, ¶¶118-27. A POSITA would modify *Kling* in one of two alternative ways. Ex-1029, ¶¶119-21. First, *Lim* would motivate a POSITA to move *Kling*’s mobile device login steps (“Display secondary login message” 413 and “Enter login and password” 414) earlier in time to coincide with the PC login steps (“Display login screen” 403 and “Enter login and password” 404), as shown in *Kling* annotated Figure 4 (above). Ex-1029, ¶134. This motivation comes from *Lim*’s teaching that “user terminals ... are very susceptible to a variety of types of malware...” (Ex-1030 ¶[0009]) and that “using a mobile terminal” for authentication “enhance[s] the security” (Ex-1030

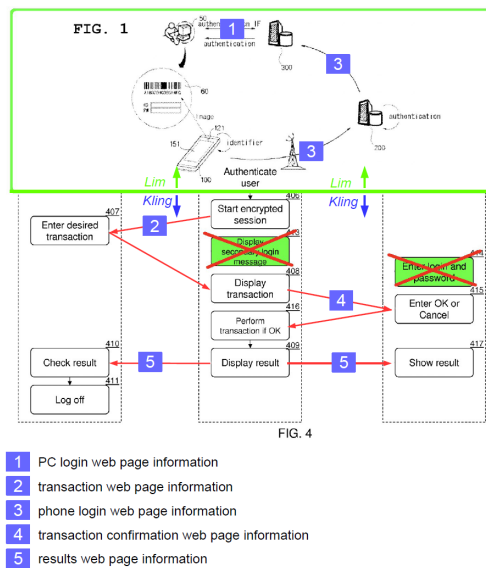
¶[0010]) where “personal information ... stored in service servers are being divulged by the hacking of external intruders” (Ex-1030 ¶[0005]).

A POSITA reading *Lim* understands that personal information such as bank information is less susceptible to hacking when it is not transmitted until after the user has logged in using two devices (the PC and the phone). Ex-1029, ¶¶134-136. This knowledge would motivate a POSITA to modify *Kling* in the manner proposed. Indeed, modifying *Kling* with *Lim*’s teaching is the simple application of a known technique (requiring a user to provide authentication information on two devices prior to “allow[ing] normal access, and provid[ing] a variety of services that can be utilized by a login user” (Ex-1030, ¶ [0077])) to a known product (online banking application) ready for improvement (*Kling*’s online banking system that otherwise exposes a user’s personal banking information on a PC that could be compromised by malware) to yield predictable results (avoiding the exposure of a user’s “personal information” (Ex-1030 ¶ [0005]) if the PC is infected by malware). Ex-1029, ¶121. Indeed, *Lim* provides express motivation to improve an online banking service (e.g., “a financial service” (Ex-1030 ¶ [0007])) such as *Kling*’s banking application. *Id.*

A POSITA would have a reasonable expectation of success in making this modification because password login schemes were well known in the art for at least a decade and nothing in *Kling* requires the login of the mobile device to take place after the encrypted session has already started. Indeed, *Kling* discloses the mobile

device accessing the banking application via a web interface or an app running on the mobile device, and a POSITA was well aware at least as of 2014 that the banking server could maintain the transaction identity from one interaction to the next (e.g. by employing cookies via the web interface or other more sophisticated connections (e.g., *Gumbula*) with the specialized application). These mechanisms would allow *Kling*'s mobile device to login prior to the encrypted session and remain available for subsequent transaction confirmation requests. Ex-1029, ¶122.

Alternatively, a POSITA would be motivated to modify *Kling* in view of *Lim*'s teaching by modifying the process illustrated in Figure 4 of *Kling* to replace the login/authentication process of *Kling* with the login/authentication process of



Lim. Ex-1029, ¶123-27. A POSITA would have understood malware was a known problem in computer network systems, particularly internet systems, at the time of the alleged invention (as disclosed by both *Kling* and *Lim*). The universal motivations to protect against malware would have motivated a POSITA to combine security

measures as proposed. Ex-1029, ¶126.

In this alternative modification, modifying *Kling* with *Lim*'s teaching is the simple application of a known technique (requiring a user to provide authentication

information on two devices prior to “allow[ing] normal access, and provid[ing] a variety of services that can be utilized by a login user” (Ex-1030, ¶ [0077])) to a known product (online banking application) ready for improvement (*Kling*’s online banking system that otherwise exposes a user’s personal banking information on a PC that could be compromised by malware) to yield predictable results (avoiding the exposure of a user’s “personal information” (Ex-1030 ¶ [0005]) if the PC is infected by malware). Indeed, *Lim* provides express motivation to improve an online banking service (e.g., “a financial service” (Ex-1030 ¶ [0007])) such as *Kling*’s banking application. Ex-1029, ¶126.

A POSITA would have a reasonable expectation of success in modifying *Kling* by substituting its login/authentication with *Lim*’s login/authentication scheme prior to starting the encrypted session (*Kling* element 406, Figure 4). In particular, *Lim* explains that after the service server determines both devices are accessible and logged in, the system “allows normal access, and provides a variety of services that can be utilized by a login user,” including “the server of a financial institution, such as a bank.” Ex-1030, ¶ [0077]. Thus, *Lim* teaches that once its authentication is successful, the normal operation of a service such as *Kling*’s banking application can proceed according to its normal operation. A POSITA understands based on this disclosure that *Lim* does not interfere with the service that it enhances. Consequently, a POSITA would expect the addition of *Lim*’s authentication to *Kling* to be

successful in improving the overall security of *Kling* and preventing the types of malware attacks *Lim* discusses. Ex-1029, ¶127.

[26d]: *Kling* in view of *Lim* teaches this element. Ex-1029, ¶¶ 128-139. *Kling* teaches to transmit distinct subsets of information to the PC (web site pages to “enter desired transaction” 507) and mobile device (“display transaction” 508) if and only if both devices are accessible by the bank server 401 (i.e., the user has logged in from both devices). Ex-1029, ¶¶ 128-129. Thus, *Kling* alone discloses this element.

Id.

PO argues *Kling* does not disclose the “if and only if” limitation. RMTA at 8-10. To the extent the Board agrees with PO, *Lim* teaches determining both devices are accessible by requiring user login at both the PC (terminal 50) and the mobile terminal 100 before transmitting any banking information. Ex-1029, ¶¶130-131. As discussed above for

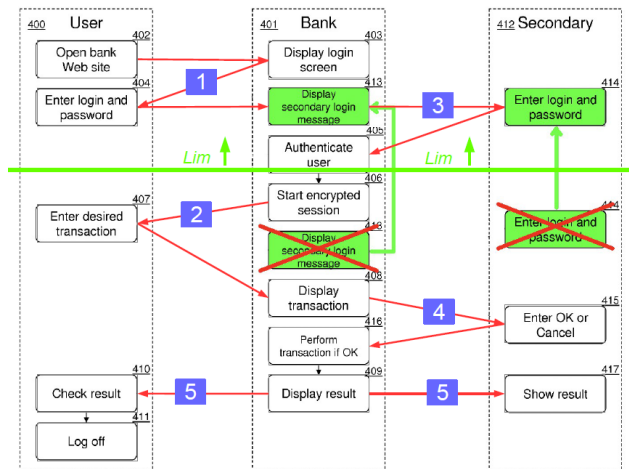


FIG. 4

- 1 PC login web page information
- 2 transaction web page information
- 3 phone login web page information
- 4 transaction confirmation web page information
- 5 results web page information

element [26c], it would be obvious to modify *Kling* as taught by *Lim* either by requiring mobile device login prior to “start encrypted session 406” or by replacing *Kling*’s authentication with *Lim*’s authentication. Ex-1029, ¶¶133-136. In either

modification, the first and second subsets are transmitted “if and only if” both devices are determined to be accessible (e.g., both have logged into the application). Ex-1029, ¶¶134, 139. Finally, the additional “thereby” clause added to element [26d] does not further limit the claims as it recites the intended results of the other steps recited in the claims. Ex-1029, ¶¶25-30.

C. Dependent Substitute Claims

Claim 27: Claim 27 is obvious in view of *Kling*, *Lim*, and a POSITA’s knowledge. Ex-1029, ¶¶140-42. In *Kling* (alone or as modified by *Lim*)³, both the transaction web page information [Arrow #2] and the results web page information [Arrow #5] generated by the bank server correspond to the “first subset of information” that is transmitted to the first device (user’s PC). The results web page

³ All references to “*Kling*” in the analysis of the dependent claims are intended to include “*Kling* alone or as modified by *Lim*.”

information [Arrow #5] corresponds to the “at least a portion of the first subset of information” because the same results information is transmitted to both the PC and the mobile device. Ex-1023, [0018]. Ex-1029, ¶141. For the “only if” limitation, a POSITA would read this limitation as a subset of the “if and only if” requirement of claim 26 because the condition is essentially the same (accessibility of both devices).

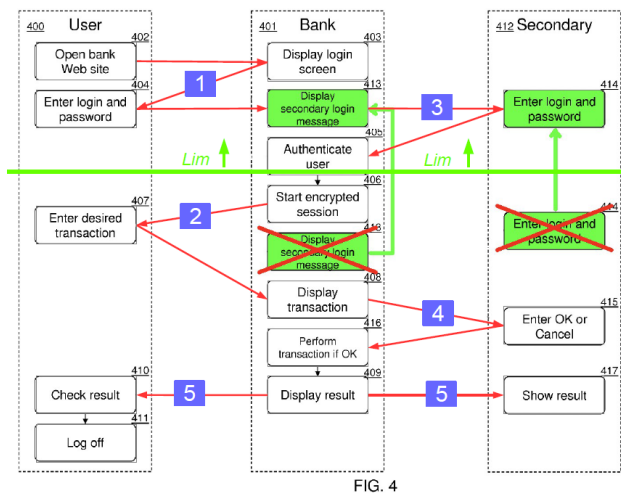


FIG. 4

- 1 PC login web page information
- 2 transaction web page information
- 3 phone login web page information
- 4 transaction confirmation web page information
- 5 results web page information

Thus, *Kling* renders this “only if” limitation obvious for the same reasons as discussed above for revised amended claim 26, namely, *Kling* and *Lim* disclose the “only if” condition. Ex-1029, ¶142.

Claim 28: As discussed above,

claim 28 lacks written description

support. Regardless, claim 28 is obvious in view of *Kling*, *Lim*, and a POSITA’s knowledge. *Kling* discloses transmitting non-sensitive information to the first device (e.g., public bank information transmitted with web page for “[e]nter desired transaction 407”) and transmitting sensitive information only to the second device. Ex-1029, ¶¶143-47. The transaction confirmation web page information [Arrow #4] comprises this “sensitive information.” *Kling* teaches the transaction confirmation web page information is only shared with the user’s mobile device to prevent

malware from capturing and modifying the desired transaction. Ex-1023, Figure 5, ¶[0019]. **Claim 29:** Claim 29 is obvious in view of *Kling, Lim*, and a POSITA's knowledge. *Kling*'s transaction confirmation web page information received at the mobile device is "more sensitive information" than the transaction web page information [Arrow #2] generated by the bank server 401 to "start encrypted session" 406 and invite the user to "enter desired transaction" 407 via the PC. It is "more sensitive" because it is the information that is required to authorize a transaction such as transferring money to another account. Ex-1029, ¶¶149-150. **Claim 30:** Claim 30 is obvious in view of *Kling, Lim*, and a POSITA's knowledge. *Kling* discloses the second device (mobile phone) utilizes a web browser access the bank server. Ex. 1023, ¶ [0005]. A POSITA would understand web browsers use HTTP protocol to determine connectivity and provide notifications, for example, an HTTP status code "503 Service Unavailable.". See Ex-1011, Abstract (Heartbeat messages), 1:56-60 (HTTP connection and status notifications), 4:44-49 ("Lost connection to the server, retrying....") Ex-1029, ¶¶151-153. **Claim 31:** Claim 31 is obvious in view of *Kling, Lim*, and a POSITA's knowledge. *Kling* discloses using the internet for the user PC and cellular for the mobile phone, which are independent electronic communication networks. Ex-1029, ¶¶154-157. **Claim 32:** Claim 32 is obvious in view of *Kling, Lim*, and a POSITA's knowledge. *Kling* discloses a user "[e]nter[s] desired transaction 407" (Ex. 1023, Fig. 4), which displays details of the

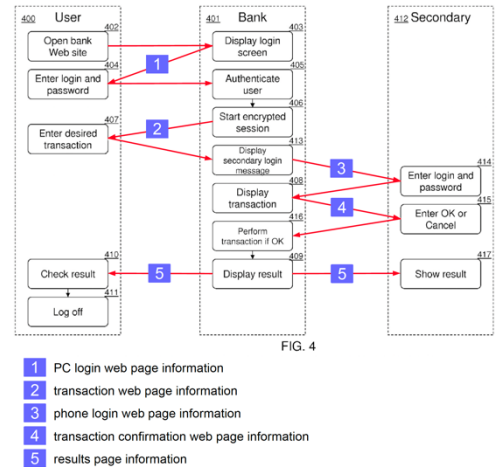
transaction. When “transfer[ing] a certain sum of money to another account” (Ex. 1023, ¶[0014]), the source account, the amount, and the destination account would display on the user’s PC and the user’s mobile phone. *See* Ex. 1023, Fig. 4 (“[d]isplay transaction 408”). Further, *Kling*’s “[s]how result 417” and “[c]heck result 410” (Ex. 1023, Fig. 4) would both display the source account, the amount, and the destination account. This information is “a graphical identifier.” Ex. 1023, ¶¶[0017]-[0018]; Ex-1029, ¶¶158-162. **Claim 34:** Claim 34 is obvious in view of *Kling*, *Lim*, and a POSITA’s knowledge. *Kling* discloses the user may log into a banking application via both the user’s PC and the user’s mobile device. Ex-1023, [0014] and [0017]. Further, *Lim* teaches the displays of the user terminal 50 and the mobile terminal 100 are being viewed exclusively by a user. Ex-1030, [0028] and Figure 1. Thus, in *Kling* (as modified by *Lin*), both devices are being viewed exclusively by the user. Ex-1029, ¶¶163-165. **Claim 35:** Claim 35 is obvious in view of *Kling*, *Lim*, and a POSITA’s knowledge. *Kling*, does not use two factor authentication. Ex-1029, ¶¶166-169. *Kling* teaches graphical indicators as discussed relative to Claim 32. **Claim 39:** Claim 39 is obvious in view of *Kling*, *Lim*, and a POSITA’s knowledge. *Kling* discloses, “rules to invoke a secondary authentication request 413,” such as “transaction amount.” Ex. 1023, ¶ [0017]. A POSITA understands a rule based on transaction amount (e.g., specifying a minimum transaction that requires secondary confirmation) would use a parameter that is the

threshold amount. Ex-1029, ¶171. **Claim 40:** Claim 40 is obvious in view of *Kling*, *Lim*, and a POSITA's knowledge. *Kling* provides the user may log into a banking application via both the user's PC and the user's mobile device. Ex-1023, [0014] and [0017]. As noted above, the transaction web page information [Arrow #2] and the transaction confirmation web page information [Arrow #4] are both generated by the bank server 401, which derives from functions within the banking application of the bank server 401. Ex-1029, ¶172.

D. Independent Substitute Claim 41

[41Pre]: *Kling* discloses this element for the same reasons as explained relative to Element [26Pre]. [41a]: *Kling* discloses this element. Ex-1029, ¶¶ 173-82. *Kling* discloses “[a] flow chart of the user's transactions 200 with a remote server 201 are shown in FIG. 2. Typically, the user would open a web site 202, in this example of a bank.” Ex-1023, [0014]. The *Kling* web site 202 corresponds to the claimed “electronically storing a set of information at a server.” A POSITA understands *Kling*'s website includes web page information stored at the server.

Additionally, *Kling* discloses the transaction web page information [Arrow #2] is “a first subset of information” generated by the bank server 401 and communicated to the user’s personal computer and the transaction confirmation web page information [Arrow #4] is



a “second subset of information” generated by the bank server 401 and communicated to the user’s mobile device. Ex-1023, Figure 4, [0017]-[0018]. **[41b]:** *Kling* discloses a remote Banking server 107, 201, 301, 401, and 501, which a POSITA understands has a processor that is programmed. Ex-1029, ¶188. **[41c]:** *Kling* discloses this element as explained for substitute claim element [26b]. Ex-1029, ¶189. **[41d]:** *Kling* and *Lim* disclose this element as explained for revised substitute claim element [26c]. Ex-1029, ¶190. **[41e]:** *Kling* and *Lim* disclose this element as explained for revised substitute claim element [26d]. Ex-1029, ¶191.

X. TAKAHASHI GROUNDS

Claims 26–35 and 37–41 are obvious in view of *Takahashi*, other prior art cited in the Petition, and the POSITA’s general knowledge (“PGK”). The *Takahashi* Grounds are all based on § 103 and include: (Ground 1) *Takahashi*+PGK, claims 26-35 and 37-41; (Ground 2) *Takahashi*+PGK+*Tsushima*, claims 26-35 and 37-41. Ex-1002 ¶¶232-255; *see also* Paper 2, 54-62.

XI. RESPONSE TO PO'S ARGUMENTS RE: *TAKAHASHI* GROUNDS

Multiple Embodiments: Patent Owner argues, “*Takahashi*’s system works with an application whether carried out on one device or two devices. Ex. 2008, ¶150.” RMTA at 18. However, prior art references are to be considered for all they teach, and *Takahashi*’s disclosure of multiple embodiments does not render the teaching of the two-device embodiment a nullity. Ex-1029, ¶¶268–69.

Login Process: PO misreads *Takahashi* as not disclosing the claimed login limitations because its “login process ... is then followed separately by an authentication process.” RMTA at 19–20. 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-1029, ¶¶270-276.

Claim 27: PO argues that “*Takahashi* fails to disclose this limitation because *Takahashi* discloses sending information to the first and second devices that is different. RMTA at 21-22. But *Takahashi*’s game server sends the same fish object image data to both the main and the sub-terminal. Ex. 1002-164-67 at ¶¶ 277.

Claim 28: PO argues, “[g]ame results for a social fishing game meant to be played with friends does not meet the Board’s construction of sensitive information.” RMTA at 22-23. However, *Takahashi* discloses playing a game with two devices

from start to finish. PO's discussion of the alternative case where a game starts with two devices and then the second device is disconnected is a different embodiment. Even so, this later embodiment is no different from the '376 Patent's disclosure of the second device disconnecting and the hole cards being shared with the first device thereafter. Ex. 1001, 5:20-26; Ex. 1002-167-69 at ¶¶261-263; Ex. 29 ¶¶278-279.

Analogous Art: PO argues *Zha* and *Takahashi* are not "analogous" prior art because "the Substitute Claims are explicitly directed toward enhancing information security." RMTA at 24-25. However, the Board's Preliminary Guidance is correct. PG at 24-25. It is wrong to assert the prior art must address the same problem (security) as the '376 Patent. Ex. 29 ¶277. Moreover, PO's attempt to change the scope of the relevant prior art by adding non-limiting verbiage to the claims through amendment (e.g., "protecting information" and "thereby" clause) would encourage mischief by patent holders faced with invalidating prior art. Regardless, *Zha* and *Takahashi* are analogous art because they address user authentication to an online application via two devices in online computer systems. Ex-1029, ¶¶280-281.

XII. TAKAHASHI GROUNDS COMBINED WITH GUI

Substitute claims 26-35 and 37-41 are alternatively unpatentable based on the *Takahashi* Grounds as modified by *Gui*'s disclosure of using multiple/different passwords with different devices. See Ex. 1002 ¶ 50 (Grounds 7-8); Ex. 29 ¶¶278-283. A POSITA would modify *Takahashi* so that the game application allows

different passwords to access the same user account where *Gui* Figure 2 shows the service (i.e., the application) handling the device authentication and different passwords for different devices. Not only does *Gui* expressly teach this approach, but this is also an example of combining prior art elements (multiple passwords in place of a single password) according to known methods to yield predictable results (allowing the same user to access a service/account from different devices). A POSITA would also find this modification to be the simple substitution of one known element (multiple password system) for another (single password system) to obtain predictable results (allowing the same user to access a service/account from different devices). Further, using multiple passwords for different devices is a predictable use of prior art elements (*Gui*'s multiple passwords) according to their established functions (allowing one user to access the same application/account with different passwords on different devices). Finally, this combination merely applies a known technique (multiple passwords for accessing the same application/account) to a known device (*Takahashi*'s online game) ready for improvement (to make it easier for users logging on with limited human interface options such as a cell phone) to yield predictable results (successful login to the same account with different passwords). Ex. 29 ¶¶282-287.

May 22, 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 May 22, 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