

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Inter Partes Review of U.S. Patent No. 9,064,376

Trial No.: IPR2023-00693

Issued: June 23, 2015

Filed: July 28, 2014

Inventor: Aviel David Rubin

Original Assignee: None

Title: Utilization of Multiple Devices to Secure Online Transactions

MAIL STOP PATENT BOARD

Patent Trial and Appeal Board

United States Patent & Trademark Office

P.O. Box 1450

Alexandria, Virginia 22313-1450

THIRD DECLARATION OF SIGURD MELDAL, Dr.Scient.

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

By:



LIST OF EXHIBITS

1001	Rubin, U.S. Patent No. 9,064,376 (“the ’376 Patent”)
1002	Reserved
1003	Prosecution History File Wrapper of the ’376 Patent (excerpts)
1004	U.S. Patent No. 9,497,565 (“ <i>Zha</i> ”)
1005	CN 2013/10674692 (“ <i>Zha Priority Application</i> ”)
1006	Certified English translation of the <i>Zha Priority Application</i>
1007	U.S. Patent Pub. No. 2015/0011318 (“ <i>Takahashi</i> ”)
1008	PCT/JP2012/007595 (“ <i>Takahashi Priority Application</i> ”)
1009	Certified English translation of <i>Takahashi Priority Application</i>
1010	U.S. Patent Pub. No. 2014/0006485 (“ <i>Tsushima</i> ”)
1011	U.S. Patent No. 9,591,083 (“ <i>Gumbula</i> ”)
1012	U.S. Patent Pub. No. 2012/0017236 (“ <i>Stafford</i> ”)
1013	U.S. Patent No. 9,330,531 (“ <i>Wakeford</i> ”)
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. No. 2012/0253841 (“’841 Application”)
1016	U.S. Patent Pub. No. 2012/0209770 (“’770 Application”)
1017	U.S. Patent Pub. No. 2014/0121015 (“ <i>Massing</i> ”)
1018	U.S. Patent Pub. No. 2006/0058088 (“ <i>Crawford</i> ”)
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 (“ <i>Kling</i> ”)

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 Patrick Traynor – February 15, 2024 (condensed)
1027	Reserved
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	Reserved
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)

LIST OF APPENDICES

Appendix D1 List of Materials Considered

TABLE OF CONTENTS

I.	INTRODUCTION	11
II.	LACK OF WRITTEN DESCRIPTION SUPPORT FOR REVISED SUBSTITUTE CLAIMS 28, 30, AND 35	11
A.	Legal Standard	11
B.	Newly-Added Limitation “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,” As Recited in Limitation [26c] and [41d] Lacks Written Description Support	12
C.	Newly-Added Limitation “the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device,” Lacks Written Description Support	13
III.	INDEFINITENESS: “THE INFORMATION DISPLAYED ON THE RESPECTIVE DEVICES” (CLAIMS 32 & 35).....	18
A.	Legal Standard	18
B.	The Phrase “the Information Displayed on the Respective Devices” in Revised Substitute Claims 32 and 35 Fail to Inform a POSITA About the Scope of the Invention.....	18
IV.	CLAIM CONSTRUCTION	20
A.	Legal Standard	20
B.	Preliminary Guidance construction of “application specific authentication information.”	21
C.	Preliminary Guidance construction of “sensitive information”	22
D.	To a POSITA, the new “thereby” clause in claims 26 and 41 simply expresses the intended result of a process step that is positively recited.....	23
V.	INFORMATION CONSIDERED.....	26

VI.	THE REVISED SUBSTITUTE CLAIMS 26-41 ARE INVALID IN VIEW OF PRIOR ART	26
A.	Legal Standard of Obviousness	27
B.	Level of Ordinary Skill in the Art	29
VII.	OVERVIEW OF CONCLUSIONS.....	31
VIII.	RECITATION OF THE REVISED SUBSTITUTE CLAIMS	34
IX.	GROUND 10: REVISED SUBSTITUTE CLAIMS 26-32, 34- 35, AND 39-41 ARE OBVIOUS OVER <i>KLING</i> AND <i>LIM</i> AND A POSITA’S KNOWLEGE	38
A.	Overview of <i>Kling</i>	38
B.	Overview of <i>Lim</i>	45
C.	Independent Substitute Claim 26.....	50
1.	[26Preamble] “A method for protecting information by transmitting information to multiple electronic devices, the method comprising:”	50
2.	[26a] “electronically storing a set of information at a server,”.....	51
3.	[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;”	53
4.	[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 application specific authentication information used on the first device is different from the application specific authentication information used on the second device;”	60

5.	[26d] “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.”	85
D.	Revised Substitute Claim 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.”	95
E.	Revised Substitute Claim 28 — “The method of claim 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”	96
F.	Revised Substitute Claim 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”	100
G.	Revised Substitute Claim 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 on the second device that the connectivity has been disrupted.”	101
H.	Revised Substitute Claim 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.”	103
I.	Revised Substitute Claim 32 — “The method of claim 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”	105
J.	Revised Substitute Claim 34 — “The method of claim 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”	108
K.	Revised Substitute Claim 35 — “The method of claim 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.”	111
L.	Revised Substitute Claim 39 — “The method of claim 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.”	114
M.	Revised Substitute Claim 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.”	115
N.	Independent Revised Substitute Claim 41	116
1.	[41Preamble] “A system for protecting information by transmitting information to multiple electronic devices, the system comprising:”	116
2.	[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”	117
3.	[41b] “a processor device programmed for:”	124
4.	[41c] “identifying a first subset of the information and identifying a second subset of the information;”	124

5.	[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;”	124
6.	[41e] “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.”	125
X.	THE PETITION GROUNDS WITH <i>ZHA</i> AS PRIMARY REFERENCE	125
A.	Obviousness under 35 U.S.C. § 103	125
1.	Revised Substitute Claims 26 and 41	126
2.	Revised Substitute Claims 27-29, 31-34, and 36-40	139
3.	Revised Substitute Claim 30	139
4.	Revised Substitute Claim 35	141
B.	Response to Patent Owner’s Arguments Related to <i>Zha</i> Grounds	143
1.	“authentication information”	143
2.	Preamble and “thereby” limitation [d]	149

3.	“sensitive information is only shared with the second device”	150
XI.	ADDITIONAL GROUNDS: <i>ZHA</i> GROUNDS COMBINED WITH <i>GUI</i>	153
XII.	THE PETITION GROUNDS WITH <i>TAKAHASHI</i> AS PRIMARY REFERENCE.....	159
A.	Obviousness under 35 U.S.C. § 103	159
1.	Revised Substitute Claims 26 and 41	159
2.	Revised Substitute Claims 27-29, 31-34, and 37-41	167
3.	Revised Substitute Claim 30	168
4.	Revised Substitute Claim 35	169
B.	Response to Patent Owner’s Arguments Related to <i>Takahashi</i> Grounds	171
1.	Takahashi discloses revised substitute claims 26-35 and 37-41	171
2.	Login process followed by an authentication process (revised substitute claim 26, limitation [c])	173
3.	Revised substitute claim 27	178
4.	Revised substitute claim 28	178
5.	<i>Zha</i> and <i>Takahashi</i> are “analogous”	179
XIII.	ADDITIONAL GROUNDS: <i>TAKAHASHI</i> GROUNDS COMBINED WITH <i>GUI</i>	180

I. INTRODUCTION

1. I have been retained by counsel for Kahoot! ASA and Kahoot EDU, Inc. as an expert witness in the above-captioned proceeding. In addition to the issues I have addressed in my first and second declarations (Exs. 1002 and 1027), I have been asked to provide my opinion about (1) whether the '376 Patent specification provides written description under 35 U.S.C. § 112 for Patent Owner's proposed claim amendment of "the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device" (revised substitute claim 28); (2) whether, for purposes of definiteness under 35 U.S.C. § 112, the phrase "the information displayed on the respective device" in revised substitute Claims 32 and 35 when read in light of the specification and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention; and (3) whether revised substitute claims 26-41 of the '376 Patent are patentable in view of the prior art.

II. LACK OF WRITTEN DESCRIPTION SUPPORT FOR REVISED SUBSTITUTE CLAIMS 28, 30, AND 35

A. Legal Standard

2. I have been advised that to satisfy the written description requirement, the disclosure of the application relied upon must reasonably convey to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.

3. I further understand from counsel that it is Patent Owner's burden to set forth written description support in the originally filed disclosure of the subject patent for each proposed substitute claim.

B. Newly-Added Limitation “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,” As Recited in Limitation [26c] and [41d] Lacks Written Description Support

4. Patent Owner seeks to amend substitute claims 26 and 41 to require that the application specific authentication information is “not authentication information specific to a device at both the first and second devices.” The proposed amendment requires that the application specific authentication information is not device specific for both the first and second devices. That is, it is not permissible for the application specific authentication information to be non-device specific for say, the first device, but be device specific for the second device. I have reviewed the portions of the '995 Application cited by Patent Owner as support for this new feature. RMTA at 3 (citing Fig. 10, ¶26, ¶33, ¶75, ¶83, ¶89, ¶90, ¶92), 6 (same); Ex. 2008 at ¶68. At best, these portions disclose that the application specific authentication information for the second device is not device specific. 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 limiting the authentication information provided by the first device.

In other words, there is no disclosure of a requirement that the application specific authentication information would not be device specific on both devices.

For the foregoing reasons, it is my opinion that there is not adequate written description support for new claim limitation [26c] and [41d] as understood and argued by Patent Owner and its expert.

C. Newly-Added Limitation “the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device,” Lacks Written Description Support

5. Patent Owner seeks to amend revised substitute claim 28 by adding the bolded, underlined words in limitation [28b]: “the second subset of the information comprises sensitive information **and the sensitive information is only shared with the second device.**”

6. I note that Patent Owner has not explained how any of the cited portions of the '995 App. actually support the amended claim limitation. Thus, it is unclear to me why or how Patent Owner believes the cited portions relate to the claims or provide written description support for the claims. I have reviewed the cited portions. My analysis of the written description support (i.e., lack of support) for the new limitation is based on the current record. Patent Owner's failure to provide any explanation related to this additional limitation makes my analysis difficult because

I am forced to guess at what Patent Owner believes the scope of the limitation to mean. I reserve the right to supplement my declaration should Patent Owner be given an opportunity to provide a claim construction for this new term.

7. Revised substitute claim 28 depends from claim 26. Revised substitute claim 26 recites “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.” Revised substitute claim limitation [28b] further provides “the second subset of the information comprises sensitive information **and the sensitive information is only shared with the second device.**” Thus, while claim 26 is couched in terms of “transmitting” the second subset of information from the server to the second device (and not the first device), claim 28 introduces a new concept, i.e., “sharing” (or not sharing).

8. Initially, I note that the word “shared,” which is used in revised substitute claim [28b], does not appear in the specification. Neither does the word “sharing.” The word “share” appears only once in the following context:

Yet another way that the two devices can remain synchronized is for the application on the first device and the application on the second device to **share** a direct communication line such as Bluetooth, WiFi, or some other way of communicating.

Ex. 1001, 6:37-41 (emphasis added). The use of the word “share” here is in the context of two devices sharing a connection, which is much different than the word “shared” in the context of the claim, which is in the context of sharing information.

Thus, the above specification passage does not reasonably convey to a POSITA that the patentee had possession of the claimed subject matter (“the sensitive information is only shared with the second device”) as of the ’376 Patent’s filing date.

9. Patent Owner argues that *Zha* does not disclose “sensitive information is only shared with the second device” because *Zha*’s “private ‘messages’ are by definition shared beyond the second device.” RMTA at 17. To support this argument, Patent Owner cites to its expert’s declaration, Ex. 2008, at ¶¶ 109-13. Dr. Traynor provides further argument on this point: “*Zha*’s private messages by definition cannot meet this limitation because they are messages between individuals and requires sharing the sensitive information beyond the second device.” Ex. 2008, ¶ 112.

10. These arguments suggest that Patent Owner and its expert understand the new limitation in revised substitute claim limitation [28b] to mean that sensitive information cannot be or have been transmitted, shared, communicated, or disclosed to any other device, at any time.

11. I disagree with PO’s arguments for reasons I discuss later in this declaration (i.e., in my discussion of the *Zha* grounds related to claim 28). However, if one were to accept PO’s argument, along with its implicit construction of “the sensitive information is only shared with the second device,” it is my opinion that this new claim limitation lacks written description support because the ’376 Patent

specification does not reasonably convey to a POSITA that the patentee had possession of the claimed subject matter as of the '376 Patent's filing date.

12. I have reviewed the '376 Patent specification, including the paragraphs Patent Owner cites as alleged written description support for new claim limitation [28b] (RMTA at p.4). 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. To the contrary, the embodiments disclosed in the '376 Patent expressly contradict Patent Owner's apparent understanding of the new claim limitation. In particular,

- A POSITA understands that hole cards (the sensitive information in the poker embodiment) are sent to the first device and shared with every player at the end of the game—this happens after the hole cards (sensitive information) are first transmitted to the second device.

After the hand is completed, when any exposed cards, such as at a showdown, are sent to the player, the hidden hole cards can be sent to the first device, so that they can be stored in hand histories that are kept on the first device. More generally, after the information has diminished value, for example because the hand is completed, the information previously only visible on the second device can be sent to the first device.

Ex. 1001, 5:56-63.

- A POSITA understands that bank transaction information (sensitive information in the banking embodiment) is shared with other devices

and individuals such as bank employees and recipients of funds transfers, and this sharing would occur after the transaction information (sensitive information) was first sent to the second device. Ex. 1001, 8:43-60 (discussing funds transfers and bill payment).

- A POSITA understands that medical records (sensitive information in the healthcare information embodiment) would be shared with medical providers. Ex. 1001, 10:23-45 (discussing medical records viewing). For example, a medical provider might view the medical records to diagnose an illness or recommend a procedure after the medical records were sent to the second device for viewing by the patient.

13. For the foregoing reasons, it is my opinion that there is not adequate written description support for new claim limitation [28b] (“the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device”) as understood and argued by Patent Owner and its expert.

III. INDEFINITENESS: “THE INFORMATION DISPLAYED ON THE RESPECTIVE DEVICES” (CLAIMS 32 & 35)

A. Legal Standard

14. I have been advised that a claim is indefinite if its claims, read in light of the specification and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.

B. The Phrase “the Information Displayed on the Respective Devices” in Revised Substitute Claims 32 and 35 Fail to Inform a POSITA About the Scope of the Invention

15. In my opinion, a POSITA would find that the phrase “the information displayed on the respective devices” does not inform a POSITA about its scope for the reasons discussed below.

16. Revised substitute claim 32 depends from revised substitute claim 26 and recites:

The method of claim 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**.

RMTA at 4-5 (emphasis added).

17. Revised substitute claim 35 depends from revised substitute claim 30, which depends from revised substitute claim 28, which depends from revised substitute claim 26, and recites:

The method of claim 1, 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**.

RMTA at 5 (emphasis added).

18. It is unclear what “the information displayed on the respective devices” refers to in this claim. On the one hand, “the information” could refer back to some previous recitation of “information” that is “displayed on the respective devices” yet neither revised substitute claim 32 or 35—or the claims on which they depend—recite displaying “information.” Revised substitute claim 26 recites various “information” including “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. It is possible that “the information displayed on the respective devices” might refer to one of these different types of recited “information,” but which one is unclear. I further note that revised substitute claims 30, 28, and 26 (from which 32 and 35 depend) do not actually recite displaying any of these types of recited “information,” which adds to the lack of clarity of this claim.

19. On the other hand, “the information displayed on the respective devices” could refer to the “graphical identifier” and the “corresponding graphical

indicator” which, according to revised substitute claims 32 and 35, are “display[ed]” on the first device and the second device, respectively. This would give the claims a different scope than if “the information displayed on the respective devices” was referring back to information recited in revised substitute claim 26. Thus, what this phrase refers to is important to understanding the claims. Neither the specification nor the file history clarify this ambiguity.

IV. CLAIM CONSTRUCTION

A. Legal Standard

20. I have been informed that in an *inter partes* review proceeding, the Patent Trial and Appeal Board gives a claim term its ordinary and customary meaning, i.e., the meaning that the term would have to a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention. I understand that the claim language, specification, and prosecution history are relevant to determine the meaning of a claim term. I understand that the prosecution history of a patent provides the record of the examination of a patent application before the U.S. Patent and Trademark Office. The prosecution history provides evidence of how the patent examiner and the inventors understood the patent application and the claims and can therefore be instructive on how to interpret the claims. My understanding is that extrinsic evidence may also be used in understanding the meaning of a claim term. Extrinsic evidence includes dictionaries, treatises, expert testimony, and prior art.

But it is my understanding that one should first look to the intrinsic evidence in construing claims. Intrinsic evidence includes the patent itself and the prosecution history.

21. My understanding is that there are at least two circumstances where the words in a patent claim may differ from and not be given their plain and ordinary meaning. One circumstance is when the applicants act as their own lexicographer by clearly setting forth a definition of a claim term that may differ from the plain and ordinary meaning it would otherwise possess. Another circumstance is when the applicant includes or provides an intentional disclaimer, or disavowal, of claim scope. My understanding is that an applicant may act as their own lexicographer, or disclaim or disavow claim scope, in either the specification or the prosecution history of the patent. My understanding is also that the applicant may act as a lexicographer, or disclaim or disavow claim scope, by making amendments to the claims during prosecution, or by making assertions to the U.S. Patent and Trademark Office about the differences between the claimed inventions and the prior art.

B. Preliminary Guidance construction of “application specific authentication information.”

22. PO’s revised amended substitute claims 26 and 41 add a new term—“application specific authentication information.” Based on the current record, the Board construed the term “application specific authentication

information” to mean “information for authentication that is specific to an application.” PG at 7-8. I apply the Board’s preliminary construction in my analysis below.

C. Preliminary Guidance construction of “sensitive information”

23. PO’s revised amended substitute claims 28 and 37 recite the term—“sensitive information.” Based on the current record, the Board gave the term “sensitive information” its ordinary and customary meaning as would have been understood by one of ordinary skill in the art, and preliminarily adopted Petitioner’s proposed construction—*See, e.g.,* Ex. 3002, Margaret Rouse, *Sensitive Information*, TECHOPEDIA, <https://www.techopedia.com/definition/25260/sensitive-information#> (last updated Sept. 26, 2012) (last visited Mar. 6, 2024) (“Sensitive information refers to privileged or proprietary information that only certain people are allowed to see and that is therefore not accessible to everyone.”). PG at 19-20.

24. I agree with the Board’s Preliminary Guidance that the plain meaning of “sensitive information” is the proper construction and that “Sensitive information refers to privileged or proprietary information that only certain people are allowed to see and that is therefore not accessible to everyone.”

D. To a POSITA, the new “thereby” clause in claims 26 and 41 simply expresses the intended result of a process step that is positively recited.

25. Patent Owner’s revised claims 26 and 41 recite, “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.” A POSITA understands that this “thereby” clause merely states an intended result of the other recited limitations in claims 26 and 41, i.e., it does not add further steps (claim 26) or structure (claim 41).

26. Claim 26 is a method claim that recites method steps. A POSITA understands that “protecting the second subset of the information not transmitted to the first device from potential malware on the first device” is the intended result of the immediately preceding steps recited in claim limitation [26d]. In particular, limitation [26d] recites the steps (1) “transmitting the first subset of the information to the first device from the server” and (2) “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.” A POSITA understands that by not transmitting information from the second subset to the first device, that information would not be susceptible to compromise by malware on the first device. In other words, if the information is not transmitted to the first device, there is no way for malware on that first device to access the information. Thus, a POSITA understands the “thereby” clause—“thereby protecting the second subset

of the information not transmitted to the first device from potential malware on the first device”—does not recite additional steps for the method of claim 26 because the capability described in the thereby clause is no more than the expected result of the preceding method steps.

27. Claim 41 is a system claim that recites structure, including steps to be carried out by “a processor device.” A POSITA understands that “protecting the second subset of the information not transmitted to the first device from potential malware on the first device” is the intended result of the other structure recited in claim limitation [41e]. In particular, limitation [41e] recites a processor device programmed to perform the following steps: (1) “transmitting the first subset of the information to the first device from the server” and (2) “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.” A POSITA understands that by not transmitting information from the second subset to the first device, that information would not be susceptible to compromise by malware on the first device. In other words, if the information is not transmitted to the first device, there is no way for malware on that first device to access the information. Thus, a POSITA understands the “thereby” clause—“thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device”—does not recite additional structure for

the system of claim 41 because the capability described in the thereby clause is no more than the intended result of the other recited structure.

28. My opinion that a POSITA would view the “thereby” claims as simply expressing the intended result of steps that are positively recited in the claims is consistent with PO’s expert’s deposition testimony. When asked about the “thereby” clause in claim limitation 26d, PO’s expert (Dr. Traynor) testified:

A. So let me just try to be clear again. This is about information isolation. And the ’376 Patent is attempting to prevent a compromised first device from gaining access to sensitive information as is explained here in 26d. That’s done by sending some subset nonsensitive information to the first device and then sending the sensitive information only to the second device. Malware cannot access or compromise the information that it cannot see.

Traynor Dep. Tr. Vol. II, 186:11-20, 184:18-186:20.

29. I agree with Dr. Traynor that malware cannot access or compromise the information that it cannot see, and that this is accomplished by sending the sensitive information only to the second device (and not the first device) according to the method steps that precede the “thereby” clause.

30. For the reasons explained above, a POSITA understands the “thereby” clause in claims 26 and 41 simply express the intended result of steps that are positively recited elsewhere in the claims (i.e., in the same limitation preceding the “thereby” clause).

V. INFORMATION CONSIDERED

31. My opinions are based on my years of education, research, and experience, as well as my study of relevant materials. In forming my opinions, I have considered the material identified in this declaration, my first and second declarations, and in the Petition.

32. I may rely upon these materials and/or additional materials to respond to arguments raised by Patent Owner. I may also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

33. My analysis of the materials is ongoing, and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to revise, supplement, or amend my opinions stated herein based on new information and on my continuing analysis of the materials provided.

VI. THE REVISED SUBSTITUTE CLAIMS 26-41 ARE INVALID IN VIEW OF PRIOR ART

34. I have been asked to provide my opinion as to whether revised substitute claims 26-41 of the '376 Patent are patentable in view of the prior art. In my opinion, these revised substitute claims are not patentable.

A. Legal Standard of Obviousness

35. It is my understanding that a claim is not patentable under 35 U.S.C. § 103 if the claimed subject matter as a whole would have been obvious to a POSITA at the time of the alleged invention. I understand that time is viewed as of the earliest effective filing date of the patent application. I also understand that an obviousness analysis must take into account the scope and content of the prior art, the differences between the claimed subject matter and the prior art, and the level of ordinary skill in the art at the time of the invention.

36. In determining the scope and content of the prior art, it is my understanding that a reference is considered appropriate prior art if it falls within the field of the inventor's endeavor. I understand the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. In addition, a reference is prior art if it is reasonably pertinent to the particular problem with which the inventor was involved. A reference is reasonably pertinent if it logically would have commended itself to an inventor's attention in considering his problem. If a reference relates to the same problem as the claimed invention, that supports use of the reference as prior art in an obviousness analysis.

37. To assess the differences between prior art and the claimed subject matter, it is my understanding that 35 U.S.C. § 103 requires that the claimed

invention be considered as a whole. I also understand that a finding of obviousness requires more than merely demonstrating that each claim element was known in the prior art. Obviousness requires showing that a person of ordinary skill in the art would have been motivated to combine the teachings of the prior art to achieve the claimed invention and would have had a reasonable expectation of success in doing so.

38. It is my understanding that the Supreme Court has recognized several rationales for combining references or modifying a reference to show the obviousness of claimed subject matter. Some of these rationales include: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to obtain predictable results; a predictable use of prior art elements according to their established functions; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

39. I understand that obviousness in an *inter partes* review must be shown by a preponderance of the evidence, which means it is more likely than not the claims are obvious.

B. Level of Ordinary Skill in the Art

40. I am informed the time of the alleged invention of the '376 Patent is June-July 2014, which corresponds to the months in which the patent applications that led to the '376 Patent were filed. Ex. 1001, [22], [60]. It is my opinion that a POSITA at the time of the alleged invention of the '376 Patent would have a bachelor's degree in electrical or computer engineering or computer science or a comparable field of study, plus approximately two years of professional experience in the field of computers or network design and security or other relevant industry experience. Additional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education.

41. In this regard, all of the technologies, techniques, methods, and components disclosed in *Zha, Takahashi, Tsushima, Gumbula, Stafford, Wakeford, Crawford, Kling, Lim, Gui*, and all other references described below, would have been within the general knowledge of such a person of ordinary skill in the art.

42. In reaching my opinion as to the POSITA's level of skill, I have considered the types of problems encountered in the art, the prior solutions to those

problems found in prior art references, the rapidity with which innovations are made, the sophistication of the technology, the level of education of active workers in the field, and my own experience working with those of ordinary skill in the art at the time of the invention.

43. The POSITA would have had knowledge of network communication, user interfaces, and distributed architectures, as well as references relating to many well-known network technologies. The state of the art at the relevant time included the teachings of the references in this declaration.

44. I am very familiar with the technology of the '376 Patent as of the June-July 2014 time frame. By 2014, I had extensive experience relating to computer and networked systems design as well as with security. As shown in my curriculum vitae and the Background and Qualifications section above, I have interacted with, and I am familiar with individuals having this level of skill at the relevant time both as a practitioner and as an educator. In particular, at the relevant time I had served as department chair of the Computer Engineering Department at San Jose State University, a major supplier of software and computer professionals to the technology industry in California. As department chair, I was responsible for the design of the curricula educating software and computer professionals, and I was thus intimately familiar with the capabilities of a POSITA at the time. Furthermore, I served as a Program Evaluator ("PEV") for the Engineering Accreditation

Commission, evaluating software and computer engineering degree programs with respect to compliance with national standards for engineering education. As a PEV, I was thoroughly familiar with the capabilities of graduates of such programs. At the relevant time I was serving as co-director of education at the NSF STC TRUST at UC Berkeley, a federal research institution focusing on security. As co-director of education my responsibilities included the transfer of knowledge from the center's research to the nation's engineering educational programs. In addition, based on my 30 years of experience in academia and industry, including in the fields of software and computer engineering and development, networked systems design and security, the acceptance of my publications and professional recognition by societies in my field, I believe that I am an expert in the art of computer and networked systems, and security. I was also at least a person of ordinary skill by the earliest possible priority date of the '376 Patent.

VII. OVERVIEW OF CONCLUSIONS

45. I have reviewed and agree with the analysis in the Petitioner's Opposition to Revised Motion to Amend. It is my opinion that each revised substitute claim would have been obvious to a person of ordinary skill in the art at the time of the alleged invention in view of the prior art cited in the Opposition to the Revised Motion to Amend and further explained in this declaration. Below is a summary of my conclusions:

- GROUND 10 – It is my opinion that revised substitute claims 26-32, 34-35, and 39-41 are unpatentable in view of U.S. Publication No. 2012/0240203 (*Kling*) (Ex. 1023) and U.S. Publication No. 2013/0023241 (*Lim*) (Ex. 1030) along with the POSITA’s knowledge.
- Petition Grounds 1-6 – It is my opinion that revised substitute claims 26-41 are unpatentable in view of *Zha* (U.S. Patent No. 9,497,565 (Ex. 1004)) along with the POSITA’s knowledge and/or other prior art references (“*Zha* Grounds”). *See* Ex. 1002 ¶ 50. More specifically, it is my opinion that Patent Owner’s amendments to substitute claims 26-41 do not overcome the *Zha* Grounds presented in the Petition, and that these substitute claims remain obvious to a person of ordinary skill in the art. My opinion is based on already-presented Grounds 1-6, further noting that a POSITA’s knowledge includes that disclosed in *Gui*, *Lipetz*, *Lim*, and *Kling*, i.e., that different passwords can be used as application specific authentication information for systems utilizing multiple devices where malware is a concern and sensitive information is to be protected.
- New Grounds based on Petition Grounds 1-6 – It is my opinion that substitute claims 26-41 are unpatentable in view of the *Zha* Grounds combined with disclosure of *Gui* that different authentication

information can be used as application specific authentication information for systems utilizing different types of devices having different human interfaces (e.g., computer vs. cellphone interfaces).

- Petition Grounds 7-8 – It is my opinion that substitute claims 26-35 and 37-41 are unpatentable in view of *Takahashi* (U.S. Patent Pub. No. 2015/0011318 (Ex. 1007)) along with the POSITA’s knowledge and/or other prior art references (“*Takahashi* Grounds”). *See* Ex. 1002 ¶ 50. More specifically, it is my opinion that Patent Owner’s amendments to substitute claims 26-35 and 37-41 do not overcome the *Takahashi* Grounds presented in the Petition, and that these substitute claims remain obvious to a person of ordinary skill in the art. My opinion is based on already-presented Grounds 7-8 alone and, in the alternative, further noting that a POSITA’s knowledge includes that disclosed in *Kling*, *Lipetz*, *Lim*, and *Gui*, i.e., that different passwords can be used as application specific authentication information for systems utilizing multiple devices where malware is a concern and sensitive information is to be protected.
- New Grounds based on Petition Grounds 7-8 – It is my opinion that substitute claims 26-35 and 37-41 are unpatentable in view of the *Takahashi* Grounds combined with the disclosure of *Gui* that different

authentication information can be used as application specific authentication information for systems utilizing different types of devices having different human interfaces (e.g., computer vs. cellphone interfaces).

VIII. RECITATION OF THE REVISED SUBSTITUTE CLAIMS

Claim	Revised Substitute Claim Language
26	[26Preamble] A method for <u>protecting information by</u> transmitting information to multiple electronic devices, the method comprising: [26a] electronically storing a set of information at a server; [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; [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 <u>using application specific authentication information</u> <u>that is not authentication information specific to a device</u> at both the first and second devices, <u>wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device</u>; [26d] if and only if both the first and second devices are determined to be accessible by the server, then: transmitting <u>[[a]]the</u> first subset of the information to the first device from the server; and transmitting <u>[[a]]the</u> 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 <u>thereby protecting the second subset of</u>

	<u>the information not transmitted to the first device from potential malware on the first device.</u>
27	[27] 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.
28	[28] 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 <u>and the sensitive information is only shared with the second device.</u>
29	[29] 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.
30	[30] 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.
31	[31] 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.
32	[32] 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.
33	[33] 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.
34	[34] The method of claim [[1]]26, wherein 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.
35	[35] The method of claim [[1]]30,

	[35a] wherein neither the first subset of information nor the second subset comprise a two factor authentication code, <u>and</u> [35b] <u>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.</u>
36	[36] 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.
37	[37Preamble] The method of claim [[1]]26, further comprising [37a] configuring the server for managing an online game, and [37b] wherein the server is configured to communicate with a plurality of devices including a first electronic device and a second electronic device, [37c] wherein the first electronic device is primarily used to play the game, and [37d] wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.
38	[38] 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.
39	[39] The 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.
40	[40Preamble] The method of claim [[1]]26, wherein [40a] the first and second subsets of information are application-specific, and [40b] wherein the first and second subsets of information derive from functions within a specific application.

41	[41Preamble] A system for <u>protecting information by</u> transmitting information to multiple electronic devices, the system comprising: [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; [41b] a processor device programmed for: [41c] identifying a first subset of the information and identifying a second subset of the information; [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 <u>using application specific authentication information</u> <u>that is not authentication information specific to a device</u> at both the first and second devices; wherein the <u>application specific authentication information used on the first device is different from the application specific authentication information used on the second device</u>; [41e] if and only if both the first and second devices are determined to be accessible by the server, then: transmitting ~~[[a]]~~<u>the</u> first subset of the information to the first device from the server; and transmitting ~~[[a]]~~<u>the</u> 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 <u>thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.</u>
----	---

IX. GROUND 10: REVISED SUBSTITUTE CLAIMS 26-32, 34-35, AND 39-41 ARE OBVIOUS OVER *KLING* AND *LIM* AND A POSITA'S KNOWLEDGE

A. Overview of *Kling*

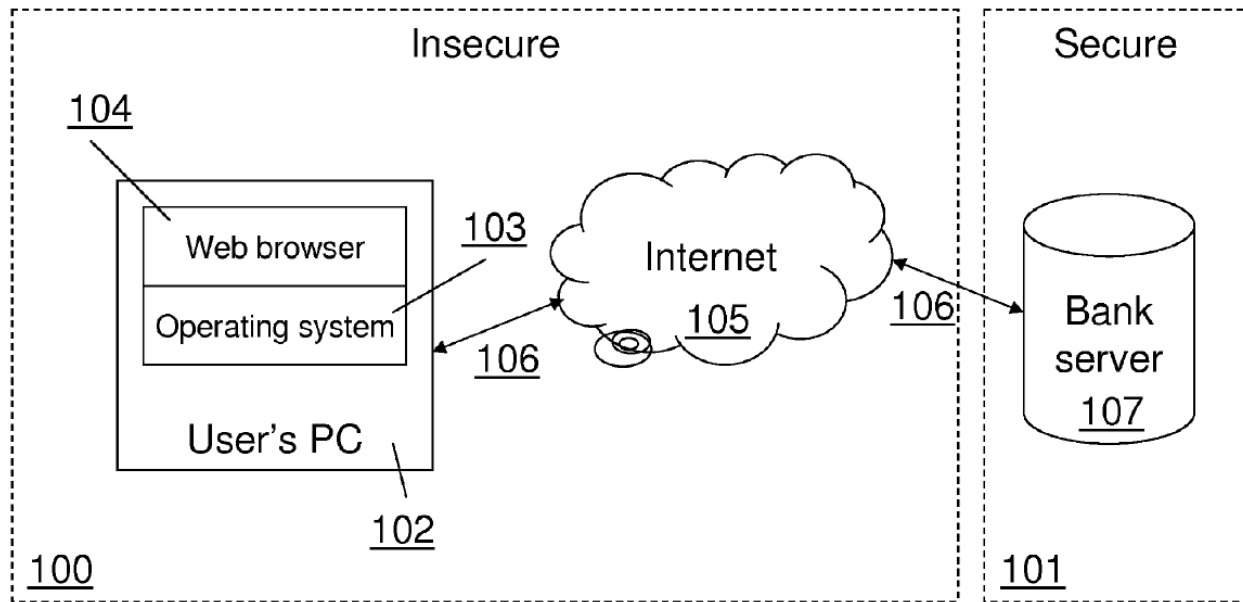
46. Counsel informs me U.S. Patent Publication No. 2012/0240203 (“*Kling*”) (Ex. 1023) is prior art under at least 35 U.S.C. § 102(a)(2) because it was effectively filed on March 16, 2011, and published on September 20, 2012, prior to the '376 Patent's filing date on July 28, 2014. Ex. 1023, [22][43]. I understand that *Kling* is listed on the face of the '376 Patent but was not cited by the Examiner during examination. Ex. 1001, [56] (References Cited).

47. *Kling* is directed to enhancing online transaction security via secondary confirmation. Ex. 1023, [54].

[A] secure transaction that is originated on one type of consumer device such as a PC is conducted to require a secondary transaction on a different device such as a mobile phone. This way an attacker faces the much harder problem of synchronously compromising two very different systems to gain control of a particular secure transaction.”

Ex. 1023, [57].

48. “Embodiments of the invention can be hosted on various computing devices but for clarity reasons we will focus on PCs and cell phones in this description.” Ex. 1023, [0013]. “Assume a user want to make a sure transaction from a local PC 102 to a remote server 107.” Ex. 1023, Fig. 1, [0013].



49. As shown in Figure 4, “the bank server 401 employs secondary authentication 412.” Ex. 1023, Fig. 4, [0017].

The secondary authentication request may be sent to a mobile device such as a cell phone that the user has previously registered with the bank server. Such a request can be sent by various means such as Internal ‘push’ data or SMS. The mobile device may open up a Web browser or invoke a specialize mobile banking app upon receipt of the server notification.

Ex. 1023, [0017].

50. A POSITA understands the last sentence in the previous quote to disclose two alternative ways the mobile device may interact with the application on the bank server. One way is through a web browser. A POSITA understands that the web browser on the mobile device would be interacting with the banking application running on bank server 401. The other way is through a banking application running on the mobile device. A POSITA understands that, in order to complete banking

transactions, the banking application on the mobile device would send and receive transaction data to and from the banking application running on bank server 401. For purposes of my analysis, I rely on *Kling*'s disclosure of the user interacting with the banking application directly through the web browser. However, my analysis would be similar in either case, the difference being that the banking application running on the mobile device may use a protocol other than HTTP to communicate with the banking application running on server 401.

51. For example, Figure 4 shows a flow chart of the user's transactions with a **remote bank server 401** via a **PC** and a **mobile device**. The **remote bank server 401** generates and transmits web pages for display on both the **PC** and **mobile device** for the user to separately provide passwords to the same bank web site application, and the server 501 authenticates the passwords. Ex. 1023, Fig. 4.

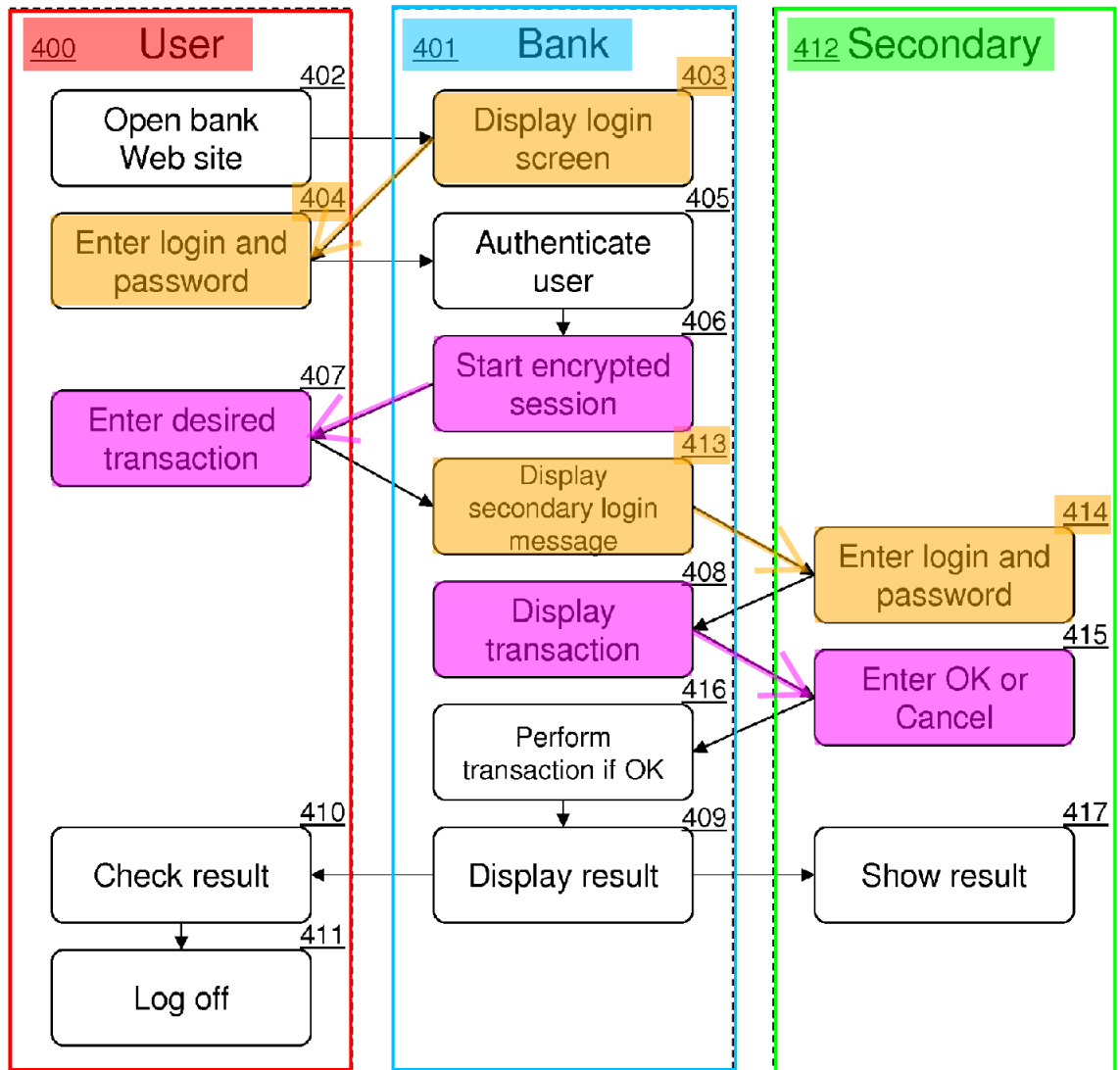


FIG. 4

52. The **remote bank server 401** generates a “**login screen**” 403 and sends it to the **PC** for display on the **PC**, and the user “**enter[s] login and password**” 404 via the **PC**. After the **remote bank server 401** “**authenticates user**” 405, the **remote bank server 401** initiates a “**start encrypted session**” 406 step, which a POSITA would understand includes establishing an encrypted communication session and sending web page information to the **PC** to enable the user’s input of the desired

transaction. Thereafter, the user “enters desired transaction” 407 based on the sufficient information sent to the user at the PC to allow the user to enter the desired transaction.

53. *Kling* explains:

Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC. Subsequently, a secure session is established between the bank server and the mobile device and the transaction is displayed for confirmation 408. The user can chose to confirm or cancel this request 415 which will terminate the secondary session. If the user confirmed the transaction the server will process it 416 and generate a result page 409 which is displayed on the user’s PC and mobile device. Otherwise, a cancellation page will be generated as the result. The user can then check the final result 410 before ending the primary session 411.

Ex. 1023, [0018].

54. I provide an annotated version of *Kling*’s Figure 4 to illustrate a POSITA’s understanding of the information sent from *Kling*’s server 401 to the user’s PC 400 and mobile phone.

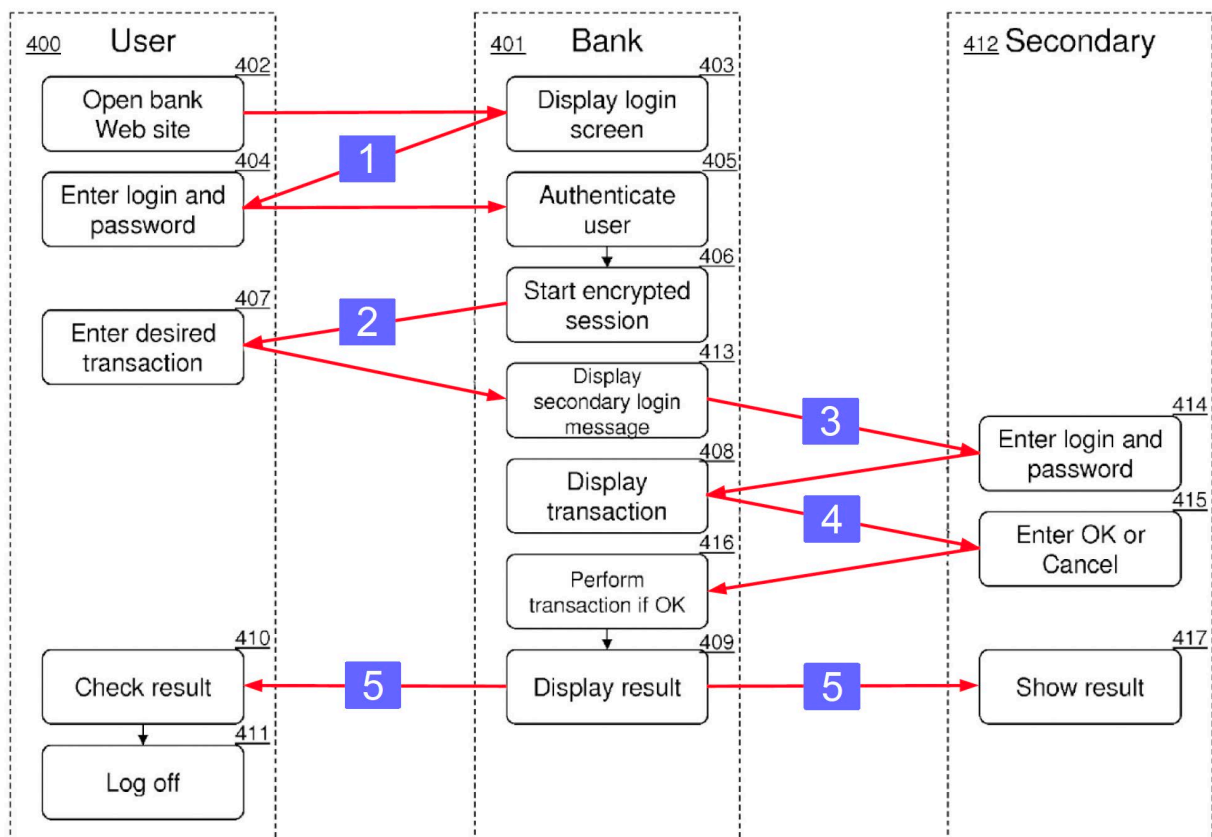


FIG. 4

- 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 page information

Ex. 1023, Figure 4 (modified and annotated)

55. Arrow #1 (between boxes 403 and 404) represents the banking application sending PC login web page information to the user's PC. A POSITA understands this to be a web page that includes at least HTML form elements for entering a username and password ("Enter login and password" in box 404). Ex. 1023 ¶¶ [0017], [0014].

56. Arrow #2 (between boxes 406 and 407) represents the banking application sending transaction web page information to the user's PC. A POSITA understands this to be a web page that presents the user with options for "enter[ing] an online banking transaction," for example, "to transfer a certain sum of money to another account." Ex. 1023, [0014].

57. Arrow #3 (between boxes 413 and 414) represents the banking application sending phone login web page information to the user's mobile phone. A POSITA understands this to be a web page that includes at least form elements for entering a username and password ("Enter login and password" in box 414). Ex. 1023, ¶¶ [0017]-[0018].

58. Arrow #4 (between boxes 408 and 415) represents the banking application sending transaction confirmation web page information to the user's mobile phone. A POSITA understands this to be a web page that includes at least (1) a summary of the transaction the user initiated on the user's PC, and (2) HTML form elements (e.g., active web buttons which include all the information necessary to confirm a financial transaction) to allow the user to either approve the transaction or cancel the transaction ("Enter OK or Cancel in box 415). Ex. 1023, ¶ [0018]. For example, if the user initiated a transfer of \$100 from their checking account to an external account, a POSITA would understand the transaction confirmation web page information sent to the user's mobile phone at Arrow #4 would include at least

the transaction amount (\$100), an identifier of the external account to which the money is to be transferred, and the HTML form elements that, when “OK” or “Cancel” are clicked, communicate the user’s desires to the banking application, including the credentials (e.g., transaction tracking ID) necessary for the banking application to trust the reply communication. *Id.*

59. Arrow #5 (between boxes 409 and 410, and between boxes 409 and 417) represents the banking application sending results web page information to both the user’s PC and mobile phone. A POSITA understands this to be a web page that includes an indication of whether the transaction was successful or not successful (e.g., cancelled). Ex. 1023, ¶ [0018].

B. Overview of *Lim*

60. Counsel informs me U.S. Patent Publication No. 2013/0023241 (“*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, prior to the ’376 Patent’s filing date on July 28, 2014. Ex. 1023, [22][43]. I understand *Lim* was not considered by the Examiner during examination. Ex. 1001, [56] (References Cited).

61. *Lim* is directed to an authentication method and system using a portable terminal. Ex. 1030, ¶ [54].

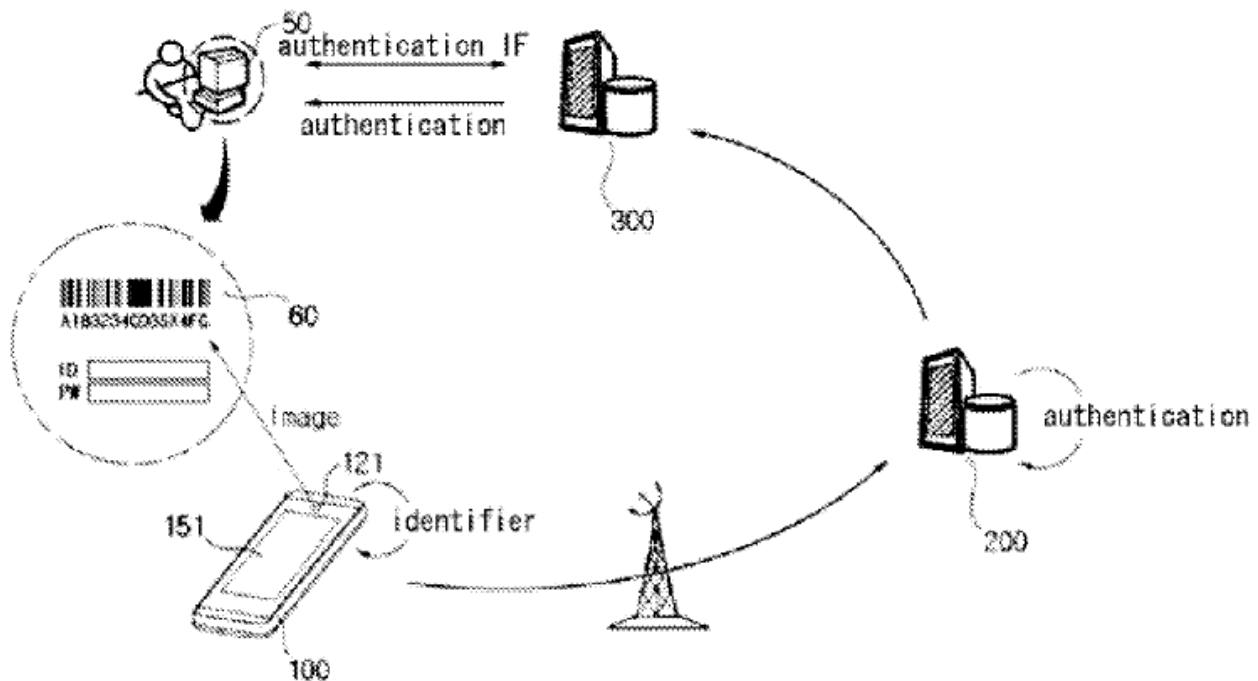
The present invention authenticates a user using identifiers and authentication information provided and displayed by the mobile terminal and the service server to and on the user terminal, in conjunction with each other. Accordingly, unless an external intruder collects information necessary for authentication from the mobile terminal, the service server, and the user terminal in the same time span, the external intruder cannot perform authentication in place of a user. The present invention can be used to process authentication in portal sites, websites of financial institutions such as banks, personal blogs, homepages, and a variety of other websites using the Internet.

Ex. 1030, [57].

62. *Lim* explains:

Referring to FIG. 1, in an authentication method according to the present invention, when the user terminal 50 connects with the service server 300 and performs authentication, for example, performs login, the service server 300 provides an authentication interface including an identifier to the user terminal 50.

Ex. 1030, ¶ [0028].



63. “The authentication interface shown in FIG. 1 includes an input box for receiving an identifier/password and an identifier 60.” Ex. 1030, ¶ [0029]. The identifier is shown as a bar code, but *Lim* discloses it can be a 1D barcode, a 2D barcode, a 3D barcode, a diagram, an image, a hieroglyphic character, a character, a special character, or a picture. Ex. 1030, ¶ [0030].

64. Once the authentication interface including the identifier 60 has been displayed on the monitor of the user terminal 50, a user captures the identifier 60 using the mobile terminal 100, and may send either the captured identifier 60 or “identifier information” that is extracted from the identifier 60 to the authentication system 200. Ex. 1030, ¶ [0033]. This extraction may be performed by “an identifier recognition module that generates identifier information by performing image processing on the identifier 60 [which module is] installed in the mobile terminal 100.” Ex. 1030, ¶ [0030].

65. The service server 300 also shares the identifier information (e.g., identifier 60) with the authentication system 200. Ex. 1030, ¶ [0037]. Then

[t]he authentication system 200 generates the identifier information from the identifier that the service server 300 has provided to the user terminal 50, and compares the identifier information with identifier information provided by the mobile terminal 100, thereby determining the validity of the identifier information. Thereafter, if it is determined that the identifier information is valid, the authentication system 200 requests authentication information from the mobile terminal 100, and the mobile terminal 100 provides the authentication information to the authentication system 200, thereby performing a final authentication process.

Ex. 1030, ¶ [0038].

66. *Lim* discloses that the authentication information from the mobile terminal 100 may be any one of: (1) an identifier/password; (2) an authentication number that was agreed with a user; (3) biometric information such as iris information, a fingerprint or a voice; and (4) a temporary approval number that the authentication system 200 issues to the mobile terminal 100. Ex. 1030, ¶¶ [0038]-[0042].

67. The “authentication information processing module” of the authentication system (Figure 3, Ex. 1030, ¶ [0066]) receives the authentication information (e.g., identifier/password) from the mobile terminal 100

and determines whether the received authentication information is identical to information stored in the database 260. If, as a result of the determination, the two pieces of information are identical to each other, the authentication information processing module 250 completes user authentication via the mobile terminal 100, and notifies the service server 300 of the success of the authentication.

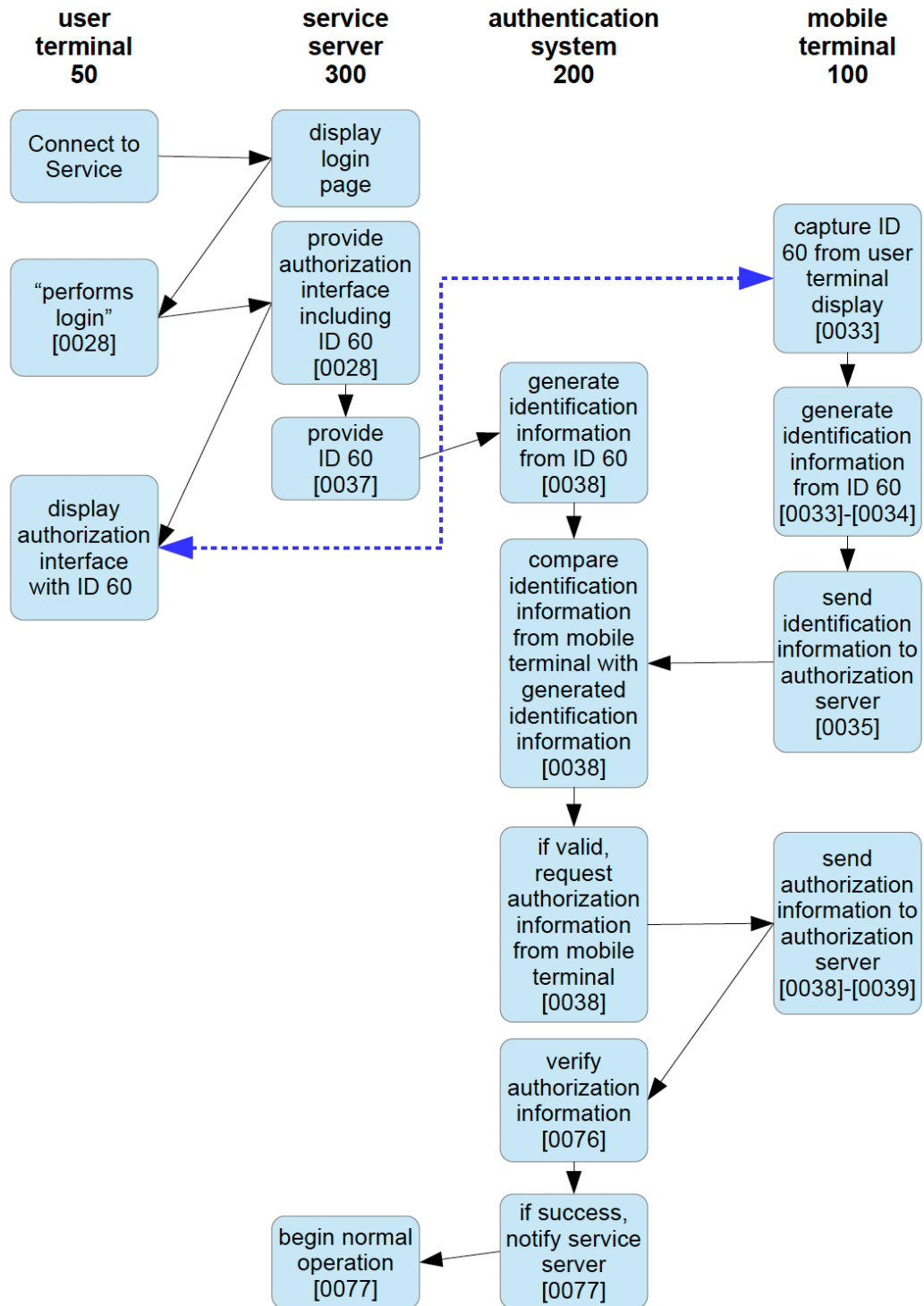
Ex. 1030, ¶ [0076].

68. *Lim* discloses that

once the success of the authentication has been notified by the authentication information processing module 250, 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].

69. I provide a flow chart of *Lim*'s operation:



C. Independent Substitute Claim 26

1. [26Preamble] “A method for protecting information by transmitting information to multiple electronic devices, the method comprising:”

70. To the extent the preamble is limiting, *Kling* and *Lim* disclose this element.

71. *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].

72. Further, *Kling* is very similar to the '376 Patent “banking” example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent “banking” example meets the preamble where it discloses a bank server 813 transmitting information to a user's computer 812 and a user's smart phone 815. Ex. 1001, Figure 8, 7:63-8:9. Similarly, *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]. Thus, *Kling* discloses this element.

73. *Lim*'s system

authenticates a user using identifiers and authentication information provided and displayed by the mobile terminal and the service server to and on the user terminal, in conjunction with each other. Accordingly, unless an external intruder collects information necessary for authentication from the mobile terminal, the service server, and the user terminal in the same time span, the external intruder cannot perform authentication in place of a user. The present invention can be used to process authentication in portal sites, websites of financial institutions such as banks, personal blogs, homepages, and a variety of other websites using the Internet.

Ex. 1030, ¶ [87].

74. As explained, *Lim* sends information to both a user terminal and a mobile terminal. Thus, *Lim* discloses this element.

2. [26a] “electronically storing a set of information at a server,”

75. *Kling* discloses this element. *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.”

76. When *Kling* published in 2012, persons of ordinary skill in the art knew a website includes web page information. Thus, where *Kling* discloses “a Web site 202, in this example of a bank,” Ex. 1023, ¶ [0014], persons of ordinary skill in the art understood the web site provides a set of sufficiently specific web page information to allow the user to enter the specific transaction the user desires to engage in.

77. To the extent Patent Owner argues *Kling* does not expressly disclose “storage” of information at the server, it is my opinion this limitation would have been obvious in view of the POSITA’s general knowledge. For example, a POSITA would understand that servers such as the *Kling* 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, such as PCs and mobile phones.

78. Evidence of the POSITA's general knowledge that servers store information the server ultimately transmits to client devices is found at least in U.S. Pub. No. 2014/0121015 to Massing et al. ("*Massing*") (Ex. 1017), as explained in my first declaration. Ex. 1002, ¶ 62.

79. Further, *Kling* is very similar to the '376 Patent "banking" example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent "banking" example meets this [26a] "electronically storing a set of information at a server" limitation where a "banking application" includes a "bank Web site" that communicates from the server (Ex. 1001, Figure 8, 7:63-8:9). Similarly, *Kling* discloses a bank server 401 with a web site banking application. Ex. 1023, Figure 4, ¶¶ [0017]-[0018]. Thus, *Kling* discloses this element.

80. *Lim* teaches a service server provides the website of a financial institution such as a bank:

[R]eference numeral "300" designates a service server that provides a variety of services to users, such as a portal site, a general website, a blog, the website of a public institution, or ***the website of a financial institution such as a bank***. Furthermore, the service server may be any of a variety of types of websites that provide information to users, personal homepages, ***a variety of websites that require login***, and specific websites that ask subscribers for their information when they subscribe to the websites.

Ex. 1030, ¶ [0024] (emphasis added).

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].

81. Thus, *Lim* disclosed this element (electronically storing a set of information at a server).

3. [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;”

82. *Kling* discloses this element. *Kling* discloses a method for identifying distinct subsets of information specific to “the Web site 202, in this example of a bank.” Ex. 1023, ¶ [0014]. In particular, *Kling* discloses:

[a]fter being prompted for a login and password 203, 204 a presumably secure transaction session is opened with the remote server 205, 206. In this session the user may enter an online banking transaction 207, for example to transfer a certain sum of money to another account” via a web page sent to the user’s PC from the server.

Ex. 1023, Figure 2, ¶ [0014]; *see also* Figure 4, ¶ [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”); Figure 5, ¶ [0019] (“The initial login process 502-507 remains the same as previously described.”).

83. Thereafter,

typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC. Subsequently, a secure session is established between the bank server and the mobile device and the transaction is displayed for confirmation 408. The user

can choose to confirm or cancel the request 415 which will terminate the secondary session.

Ex. 1023, ¶ [0018].

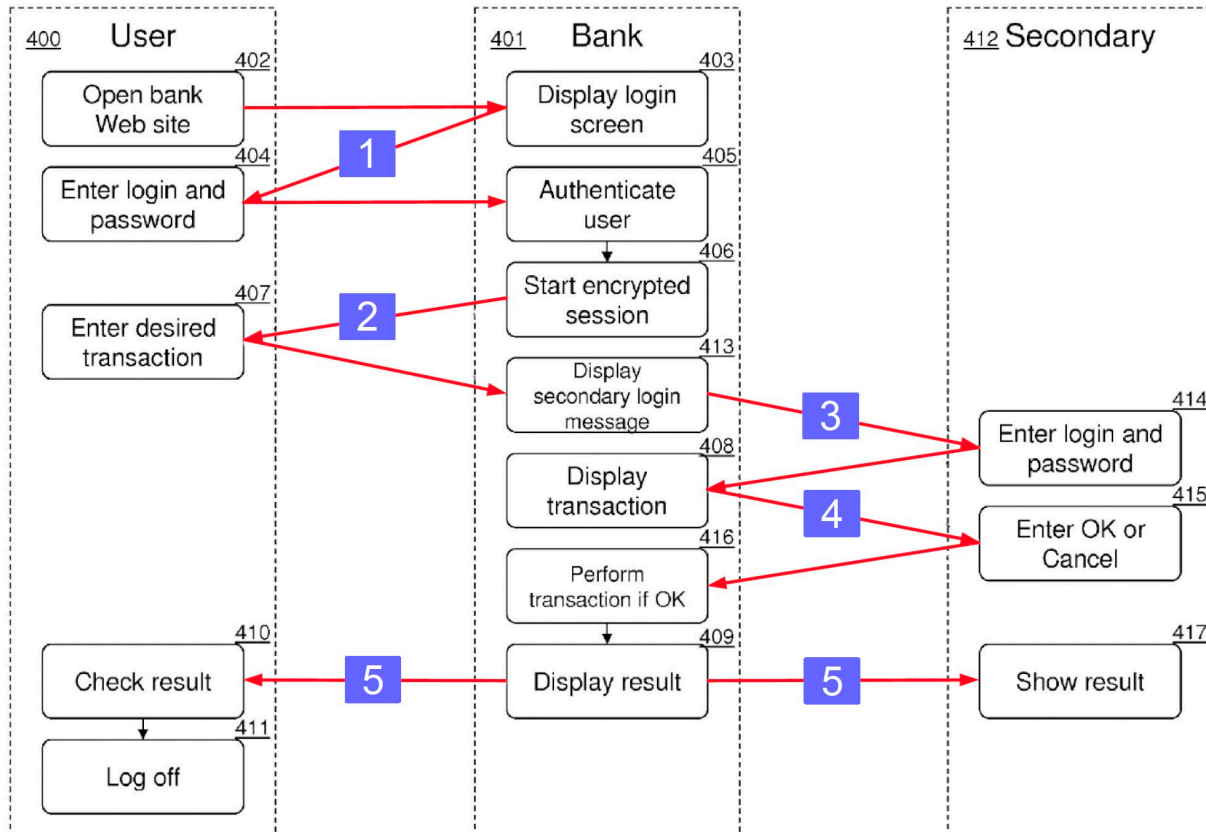


FIG. 4

- 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 page information

Ex. 1023, Figure 4 (annotated).¹

¹ Subsequent citations to “Arrow #X” for the *Kling* reference refer to the arrows in this annotated figure.

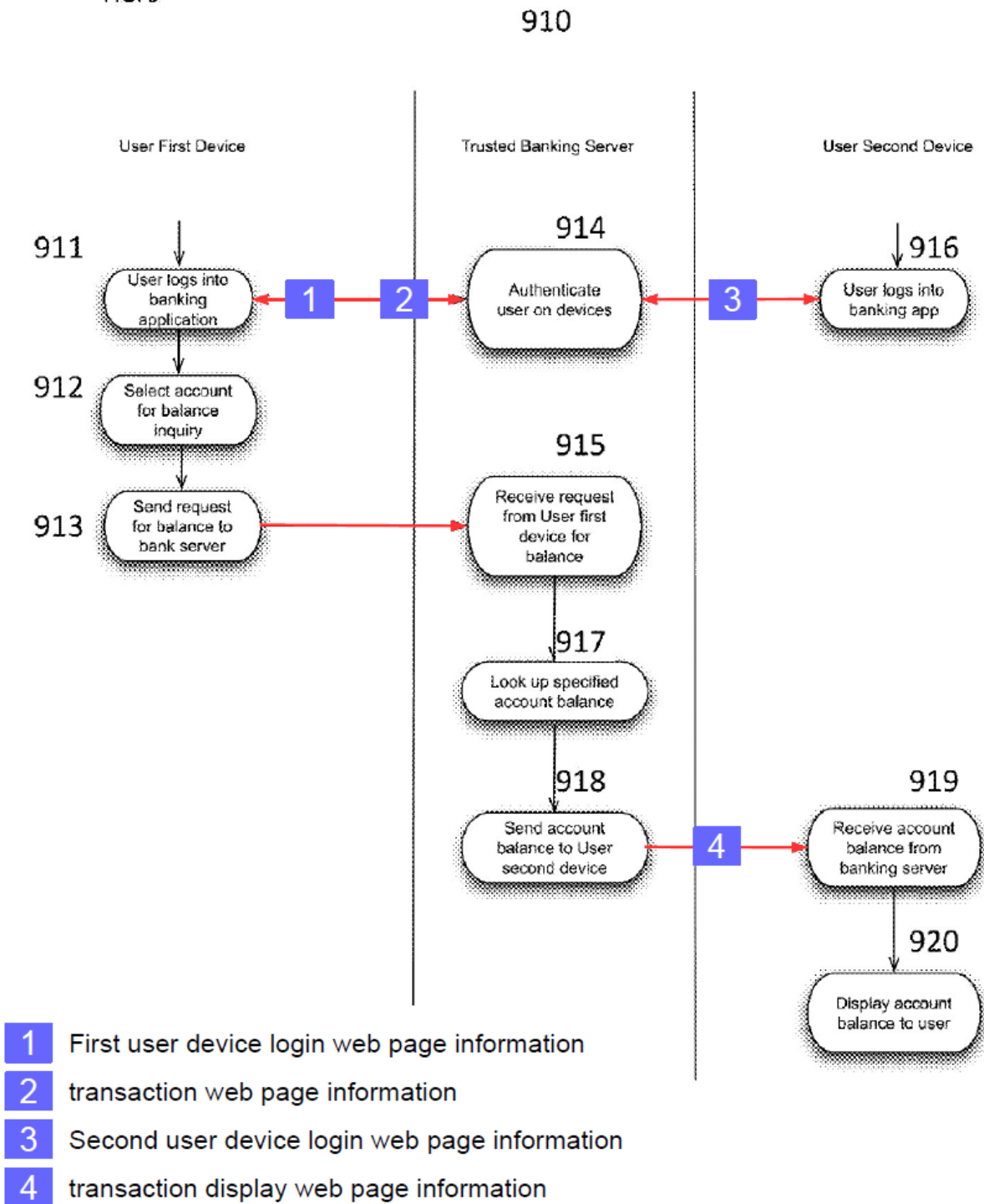
84. First, the transaction web page information [Arrow #2] sent to the user's PC for the user to "enter desired transaction 407" corresponds to the claimed "first subset of information." Second, the transaction confirmation web page information [Arrow #4] sent to the mobile device to display the transaction 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.

85. Further, *Kling* is very similar to the '376 Patent "banking" example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent "banking" example meets this [26b] "identifying a first subset of the information and identifying a second subset of the information . . ." limitation where a POSITA would understand the "bank Web site" has stored web page information on the Trusted Banking Server. *Kling* teaches a POSITA that transaction web page information [Arrow #2] is sent from the Trusted Bank Server to the User First Device for the user to "select account for balance inquiry" 914. Ex. 1001, Figure 9, 9:65-67. The transaction web page information [Arrow #2] is "a first subset of information" generated by the banking application at the Trusted Bank Server and communicated to User First Device. *Kling* also teaches a POSITA that transaction display web page information [Arrow #4] is sent from the Trusted Bank Server to the User Second Device for the user to "receive account

balance from banking server” 919. Ex. 1001, Figure 9, 10:7-9. The transaction display web page information [Arrow #4] is a “second subset of information” generated by the banking application at the Trusted Bank Server and communicated to the User Second Device.

86. Further, my annotations to Figure 9 of the '376 Patent (below) show the transaction web page information [Arrow #2] is “a first subset of information” generated by the “Trusted Banking Server” and communicated to the “User First Device” and the “transaction display web page information” [Arrow #4] is a “second subset of information” generated by the “Trusted Banking Server” and communicated to the “User Second Device.” Ex. 1001, Figure 8, 7:63-8:9. In the '376 Patent, the transaction web page information [Arrow #2] relates to a transaction for getting an account balance and it includes the information necessary to allow the user to initiate the balance query as the transaction.

FIG. 9



Ex. 1001, Figure 9, 9:65-10:9 (annotated).²

87. Similarly, *Kling* discloses to a POSITA 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.

² Subsequent citations to “Arrow #X” for the ’376 Patent refer to the arrows in this annotated figure.

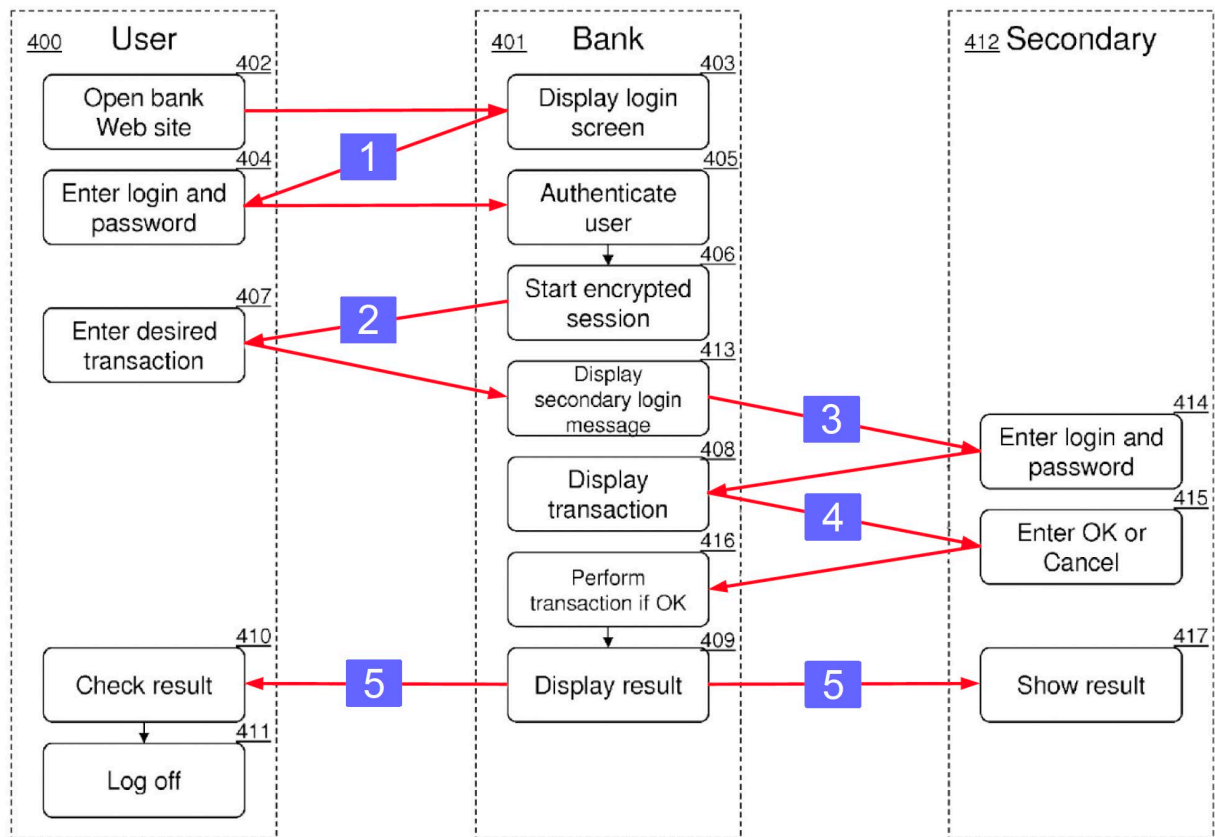


FIG. 4

- 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 page information

Ex. 1023, Figure 4 (annotated), [0017]-[0018].

4. [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 application specific authentication information used on the first device is different from the application specific authentication information used on the second device;”

88. As noted above, the Board preliminarily construed “application specific authentication information” to mean “information for authentication that is specific to an application.” PG at 7-8. Both *Kling* and *Lim* teach this limitation.

89. *Kling* teaches the [26c] limitation where a user separately logs into the banking web site application via both the PC and the mobile device using different passwords.

90. In particular, *Kling* teaches, on a PC, “the user would open a Web site 202, in this example of a bank, [and be] prompted for a login and password 203, 204.” Ex. 1023, Figure 2, [0014]; Fig. 4, [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”); Figure 5, [0019] (“The initial login process 502-507 remains the same as previously described.”).

91. Also, to the mobile device, “the bank server generates a secondary confirmation request 513, 514” (Ex. 1023, [0019]) comprising “display secondary login message 513” for the user to “enter login and password 514.” Ex. 1023, Figure

5. “Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.” Ex. 1023, [0018]. For the user’s PC 400, *Kling* expressly shows the bank server 401 “authenticates user” on the PC 400 at step 405 after the user has “enter[ed] login and password” via the PC 400 at step 407. For the user’s mobile device (a POSITA understands the steps taken by the mobile device are illustrated in the right column of Figure 4 labeled “secondary 412”), *Kling* does not expressly show an authentication step by the server, but a POSITA would understand the server similarly “authenticates user” on the mobile device after the user has “enter[ed] login and password” via the mobile device at step 414. Only after authentication via step 414 does the bank server 401 “display transaction” at step 408. A POSITA would understand that *Kling* would not display the transaction on the mobile device unless it had authenticated the user on the mobile device. Thus, the *Kling* bank server 401 determines whether both the user’s personal computer in possession of and being directly operated by a user and a mobile device also in possession of and being directly operated by the user are accessible over at least one electronic communications network based on the user being logged into the application using login and password at both the user’s personal computer and mobile device, wherein the login and password used on the user’s personal computer is different from the login and password used on the mobile device. Ex. 1023, Figure 4, ¶¶ [0017]-[0018].

92. The *Kling* bank server 401 generates both the PC and mobile device web pages for the user to separately provide passwords to the same banking application, and the server 401 authenticates the passwords. Ex. 1023, Figure 4. First, the bank server 401 generates a “display login screen 403” (PC login web page information [Arrow #1]) and sends it to the user’s PC, so the user may “enter login and password 404” via the user’s PC. *Id.* The bank server 401 receives the user’s login and password so as to “authenticate user 405.” *Id.* Second, the bank server 401 generates a “display secondary login message 413” (phone login web page information [Arrow #3]) and sends it to the mobile device, so the user may “enter login and password 414” via the mobile device. *Id.*

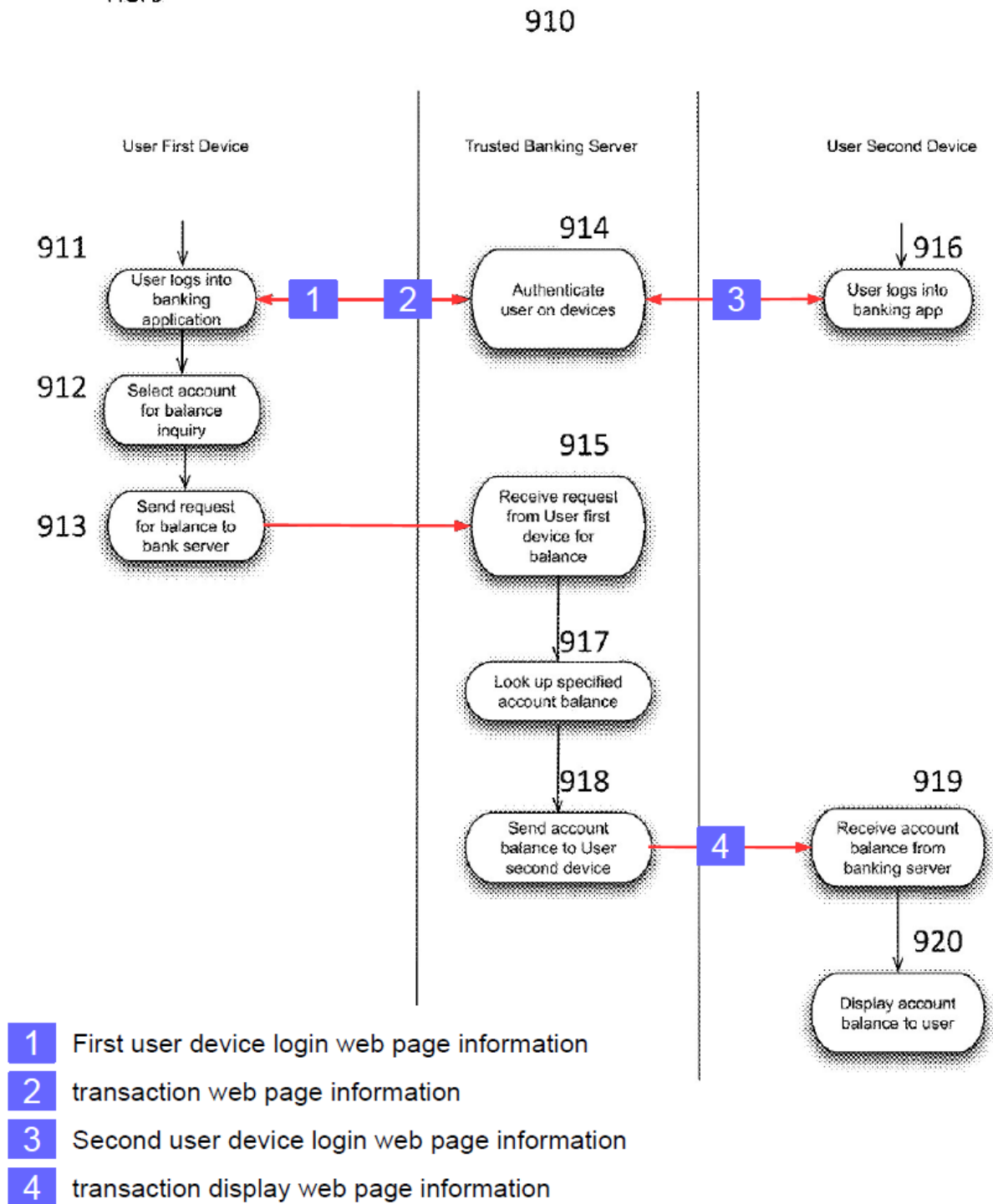
93. Thus, the *Kling* bank server 401 “determine[s] . . . whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information at both the first and second devices,” as claimed.

94. The *Kling* bank server 401 allows the user to enter different passwords on the PC and the mobile device. Ex. 1023, Figure 5. “Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.” Ex. 1023, ¶ [0018]. Thus, the *Kling* bank server 401 teaches, “the

application specific authentication information used on the first device is different from the application specific authentication information used on the second device,”
as claimed in amended claims 26 and 41.

95. Further, *Kling* is very similar to the '376 Patent “banking” example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent “banking” example meets this [26c] “determining at the server . . .” limitation where the “Trusted Banking Server” logs in the user on both a User First Device and a User Second Device, using different passwords. Ex. 1001, Figure 9, 9:65-10:9. The Trusted Banking Server sends first user device login web page information [Arrow #1] to the User First Device and the “user logs into banking application” at step 911. The Trusted Banking Server also sends second user device login web page information [Arrow #3] to the User Second Device and the “user logs into banking app” at step 916. The Trusted Banking server “authenticates user on devices” at step 914.

FIG. 9



Ex. 1001, Figure 9, 9:65-10:9. “As illustrated in FIG. 9, using a first device, a user logs into a banking application (911), selects an account for balance inquiry (912),

and sends a request for a balance to a bank server (913). Using a second device, the user logs into a banking application (916). A banking server authenticates the user on the two devices (914).” Ex. 1001, 9:65-10:3. Thus, the ’376 Patent “banking” example meets this [26c] “determining at the server . . .” limitation.

96. Similarly, *Kling* discloses the bank server 401 authenticates the user on both the user’s personal computer and the user’s mobile device, using different passwords.

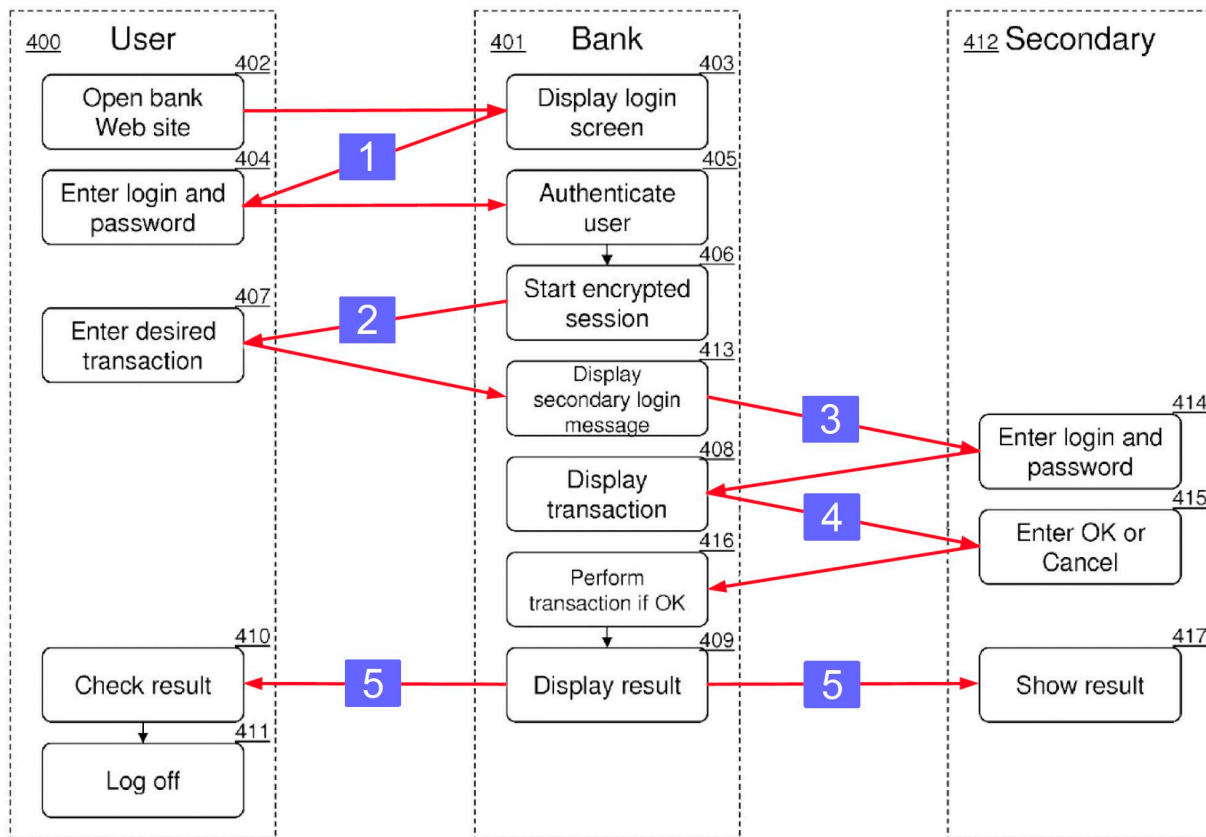


FIG. 4

- 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 page information

97. The *Kling* bank server 401 generates web pages for both the user PC and user's mobile device for the user to separately provide passwords to the same banking application, and the bank server 401 authenticates the passwords. Ex. 1023, Figure 4. First, the bank server 401 generates a "display login screen 403" (PC login web page information [Arrow #1]) and sends it to the user's PC, so the user may "enter login and password 404" via the user's PC. *Id.* The bank server 401 receives

the user's login and password so as to "authenticate user 405." *Id.* Second, the bank server 401 generates a "display secondary login message 413" (phone login web page information [Arrow #3]) and sends it to user's mobile device, so the user may "enter login and password 414" via the user's mobile device. *Id.* "Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC." Ex. 1023, [0018].

98. Thus, the *Kling* bank server 401 "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 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," as claimed. Ex. 1023, Figure 4, ¶¶ [0017]-[0018]. Thus, *Kling* discloses this element.

99. Patent Owner argues, "*Kling* discloses using authentication information specific to a device, which is contrary to 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.” RMTA at 9. I disagree.

100. Revised amended claim 26 recites, “determining . . . based on the first user being logged into the application using application specific authentication information **that is not authentication information specific to a device.**” Revised amended claim 26 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). Rather, revised amended claim 26 merely requires that the application specific authentication information *being used by the user* not be specific to a device. *Kling* teaches a user being logged into a bank web site using “login” and “password,” which is not specific to a device, which corresponds to revised amended claim 26[c].

101. Patent Owner further argues, “*Kling*’s disclosure directs the user to log into their mobile device with a different password, and not *the application.*” RMTA at 10. I disagree. With reference to Figure 2, *Kling* teaches, on a PC, “the user would open a Web site 202, in this example of a bank, [and be] prompted for a login and password 203, 204” to open a secure transaction session with the remote server 205, 206. Ex. 1023, Figure 2, ¶ [0014].

102. Figure 2 describes step 205 as “Authenticate user.” Ex. 1023, Figure 2. With reference to Figure 4, *Kling* teaches login on a user PC is the same as Figure

2, but additionally teaches “secondary authentication 412” for the mobile device. Ex. 1023, ¶ [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”); Figure 5, [0019] (“The initial login process 502-507 remains the same as previously described.”). “The secondary authentication request may be sent to a mobile device such as a cell phone that the user has previously registered with the bank server.” Ex. 1023, ¶ [0017].

103. Also, to the mobile device, “the bank server may decide, based on a set of rules to invoke a secondary authentication request 413” (Ex. 1023, ¶ [0017]) comprising “display secondary login message 413” for the user to “enter login and password 414.” Ex. 1023, Figure 4. “The mobile device may open up a Web browser or invoke a specialized mobile banking app upon receipt of the server notification.” Ex. 1023, ¶ [0017].

104. It is in this context that Kling states, “Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.” Ex. 1023, ¶ [0018]. A POSITA would understand *Kling* teaches the user logs into the bank web site via an open web browser or specialized mobile banking app on the mobile device.

105. *Kling* does not teach the user logs into the mobile device itself, as Patent Owner incorrectly suggests. To the contrary, a POSITA understands that even though *Kling* uses the loose language “[t]ypically the user would be prompted to log

into the mobile device,” that sentence means that the user would be prompted to log into the bank server using the mobile device. 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 was 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].

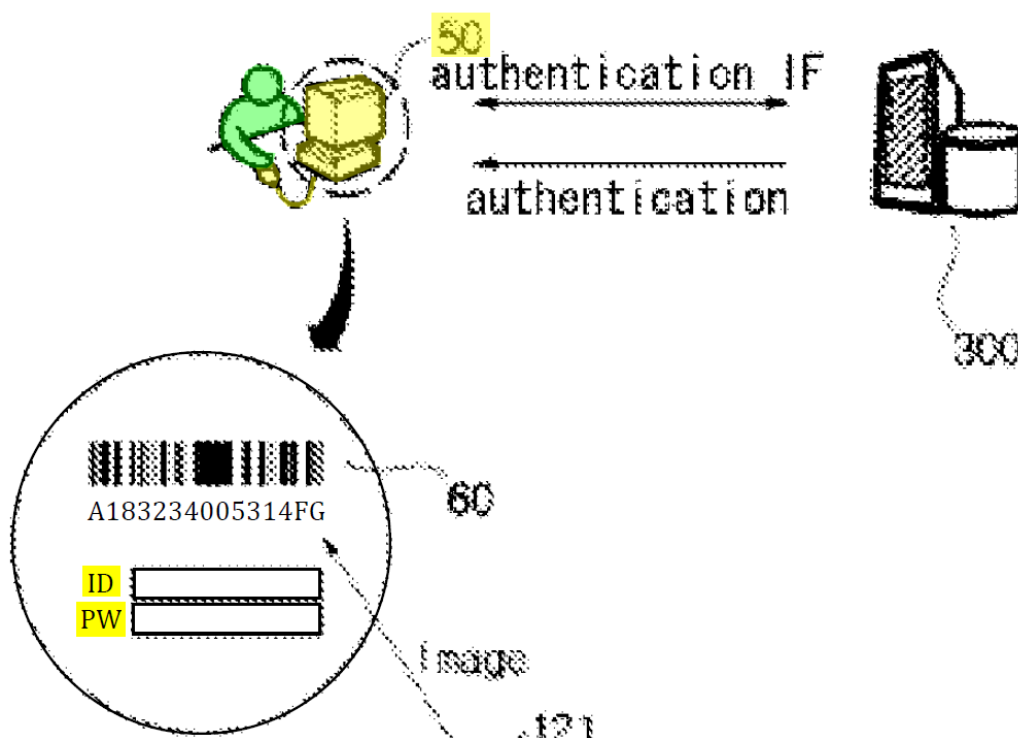
106. *Lim* also teaches limitation [26c] where a user logs into and is authenticated on both a user terminal and a mobile terminal.

107. In particular, *Lim* teaches, “determining at the server [service server 300] whether both a first device [user terminal 50] in possession of and being directly operated by a first user and a second device [mobile terminal 100] also in possession of and being directly operated by the first user are accessible over at least one electronic communications network [Internet] based on the first user being logged

into the application [bank website] using application specific authentication information that is not authentication information specific to a device [first device: “performs login” [0028]; second device: “provides authentication information” [0038]] at both the first and second devices [user terminal 50 and mobile terminal 100], wherein the application specific authentication information used on the first device is different [first device: “performs login” [0028] via “identifier/password” [0029]; second device: “provides authentication information” [0038] in form of “an identifier/password” [0039]; “an authentication number that was agreed with a user” [0040]; or “biometric information such as iris information, a fingerprint, or a voice” [0041]] from the application specific authentication information used on the second device [mobile terminal 100],” as claimed in the [26c] limitation. A POSITA understands 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 *Lim*’s first device (user terminal 50) is the same or different from the identifier/password used to authenticate the second device (mobile terminal 100), a POSITA knows based on *Kling* that they “ideally” should be different. See Ex. 1030; Ex. 1023, ¶[0017].

108. Regarding authenticating the user of a “first device,” *Lim* teaches a service server 300 determines whether a user terminal 50 is in possession of and

being directly operated by a first user because the user “performs login” [0028] and receives an “authentication interface.” Ex. 1030, ¶ [0028]. Figure 1 of *Lim* shows a user seated in front of a desktop computer identified as “user terminal 50.” The user has his hand on the mouse of the desktop computer, user terminal 50, which shows user terminal 50 is clearly “in possession of and being directly operated by” the user.



109. “The authentication interface shown in Figure 1 includes an input box for receiving an identifier/password and an identifier 60.” Ex. 1030, ¶ [0029]. *Lim* teaches a user to login to a bank website via a user terminal 50 communicating over the Internet with a service server 300 using an identifier/password. *See* Ex. 1030, ¶¶ [0024], [0028], [0029], [0087]. Thus, the service server 300 determines whether user terminal 50 is in possession of and being directly operated by the user and being

directly operated by the user is accessible over the Internet based on the user being logged into the bank website using identifier/password information. *See* Ex. 1030. This identifier/password authentication information disclosed by *Lim* is not device specific as they can be used on “any user terminal that allows an identifier to be captured by the camera 121 of the mobile terminal 100...” Ex. 1030, ¶ [0081].

110. Regarding authenticating the user on a “second device” (i.e., the mobile terminal), *Lim* teaches a service server 300 determines a second device [mobile terminal 100] is also in possession of and being directly operated by the same user by displaying an authentication interface on the monitor of the user terminal 50 so the user can take a picture of the displayed identifier 60 with her mobile device 100 and then use the identifier 60 to initiate login via the mobile device 100.

Once the authentication interface including the identifier 60 has been displayed on the monitor of the user terminal 50, a user captures the identifier 60 using the mobile terminal 100, and may send the captured identifier 60 to the authentication system 200.

Ex. 1030, ¶ [0033]. Alternatively, the mobile terminal may send “identifier information” that is extracted from the identifier 60 to the authentication system 200.

Ex. 1030, ¶ [0033].

The service server 300 also shares the identifier information (e.g., identifier 60) with the authentication system 200. Ex. 1030, ¶ [0037]. Then

[t]he authentication system 200 generates the identifier information from the identifier that the service server 300 has provided to the user terminal 50, and compares the identifier information with identifier

information provided by the mobile terminal 100, thereby determining the validity of the identifier information. Thereafter, if it is determined that the identifier information is valid, the authentication system 200 requests authentication information from the mobile terminal 100, and the mobile terminal 100 provides the authentication information to the authentication system 200, thereby performing a final authentication process.

Ex. 1030, ¶ [0038].

111. The user performs login via the mobile terminal 100 by providing authentication information that can be

any one of the following: [1] an identifier/password, [2] an authentication number that was agreed with a user, [3] biometric information such as iris information, a fingerprint, or a voice, and [4] a temporary approval number that the authentication system 200 issues to the mobile terminal 100.

Ex. 1030, ¶¶[0038]-[0042].

112. A POSITA understands that at least the first three types of authentication information disclosed by *Lim* (i.e., identifier/password, a user-specific authentication number, or a user's biometric information) are not device specific. An identifier/password is user-specific and can be used on any mobile device. An authentication number that was agreed with a user is user-specific and can also be used on any mobile device. Biometric information is user-specific and can also be used on any mobile device.

113. The “authentication information processing module” of the authentication system (Figure 3, Ex. 1030, ¶ [0066]) receives the authentication information (e.g., identifier/password) from the mobile terminal 100

and determines whether the received authentication information is identical to information stored in the database 260. If, as a result of the determination, the two pieces of information are identical to each other, the authentication information processing module 250 completes user authentication via the mobile terminal 100, and notifies the service server 300 of the success of the authentication.

Ex. 1030, ¶ [0076].

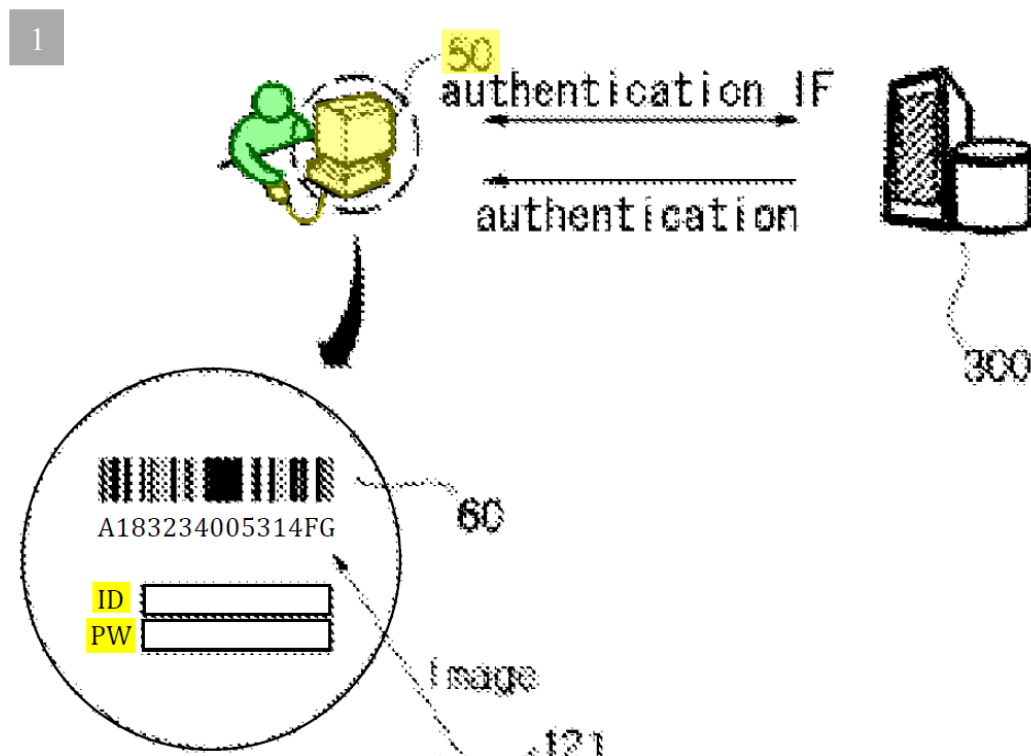
114. “Once the success of the authentication has been notified by the authentication information processing module 250, the service server 300 determines that the user terminal 50 has been successful in the authentication, allows normal access, and provides a variety of services that can be utilized by a login user.”

Ex. 1030, ¶ [0077].

115. Thus, it is determined at the server (i.e., the hardware on which service server 300 executes) that a first device [user terminal 50] and a second device [mobile terminal 100] are both in possession of and being directly operated by the same user and are accessible over at least one electronic communications network (e.g., wired or wireless network (Ex. 1030, ¶ [0027])) based on the user being logged into the application [“a variety of services that can be utilized by a login user”] using application specific authentication information that is not authentication information specific to a device.

116. *Lim* teaches the application specific authentication information used on the first device is different from the application specific authentication information used on the second device. For the first device [user terminal 50], *Lim* teaches the

user “performs authentication, for example, performs login.” Ex. 1030, [0077]. Further, “the authentication interface shown in FIG. 1 includes an input box for receiving an identifier/password and an identifier 60,” which allows the user to “perform login” by entering a user identifier and a user password via the user terminal 50. This identifier/password authentication information disclosed by *Lim* is not device specific as they can be used on “any user terminal that allows an identifier to be captured by the camera 121 of the mobile terminal 100...” Ex. 1030, ¶ [0081].



117. For the second device [mobile terminal 100], *Lim* teaches the user performs login via the mobile terminal 100 by providing “authentication information [that] may be any one of the following: [1] an identifier/password, [2] an

authentication number that was agreed with a user, [3] biometric information such as iris information, a fingerprint, or a voice, and [4] a temporary approval number that the authentication system 200 issues to the mobile terminal 100.” Ex. 1030, ¶¶ [0038]-[0042]. Thus, *Lim* expressly teaches different application specific authentication information being used on the two devices. Thus, *Lim* discloses element [26c].

118. It would have been obvious to modify *Kling* to have the bank server determine whether both the first and second devices are in possession of and directly operated by the user based on the user logging into the application on both the user PC and secondary mobile phone using application specific authentication information that is not specific to a device, as taught by *Lim*. Counsel has informed me that any need or problem known in the field of endeavor at the time of the invention and addressed by the patent can provide a reason for combining the elements in the manner claimed. Counsel has also informed me that universal motivations to improve technology within a particular field can provide a motivation to combine even absent any hint or suggestion in the references themselves. A POSITA would modify *Kling* in one of two alternative ways.

119. The teachings of *Lim* would have motivated a POSITA to modify *Kling*’s bank server’s implementation of the process illustrated in Figure 4 to simply require the user to login via the secondary mobile phone prior to starting the

encrypted session. With this modification, *Kling*'s bank server determines whether both devices in possession of and being directly operated by a user are accessible based on the user being logged in, as claimed.

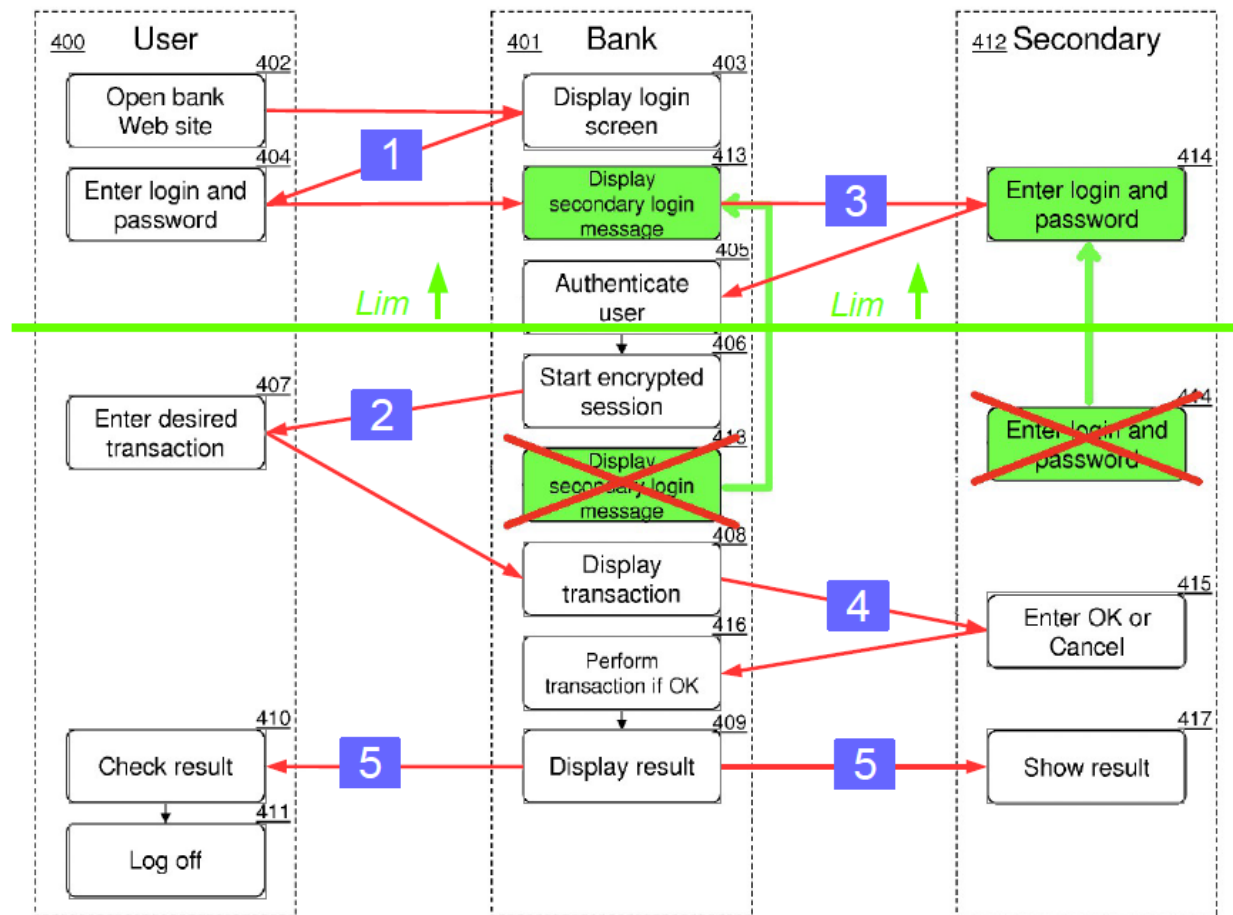


FIG. 4

- 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

A POSITA would have been motivated to modify *Kling* to move the login steps associated with the secondary mobile phone (“Display secondary login message”

413 and “Enter login and password” 414) to coincide with the steps associated with the login steps associated with the user PC (“Display login screen” 403 and “Enter login and password” 404). *Kling* teaches to protect banking transactions from malware—“As consumer online transactions such as for electronic banking are becoming much more widespread so are the incidents of compromised accounts and associated losses. In particular, consumers are likely to use very insecure platforms such as PCs and mobile phones which are prone to malware attacks.” Ex. 1023, [0003]. Similarly, *Lim* teaches to protect banking transactions from malware—“even if the user terminal 50 is attacked by a hacker or malware and therefore the identifier is stolen, it is not possible to perform any authentication related to a user using the identifier” [0044] . . . which protects transactions with “the website of a financial institution such as a bank” [0024]. A POSITA would have understood malware was a known problem in computer network systems, particularly Internet systems, at the time of the alleged invention. The universal motivations to protect against malware would have motivated a POSITA to combine security measures. Thus, a POSITA would have been motivated to modify *Kling* to authenticate the user via login on both the user PC and the secondary mobile phone, as taught by *Lim*.

120. Motivation to modify *Kling* also 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

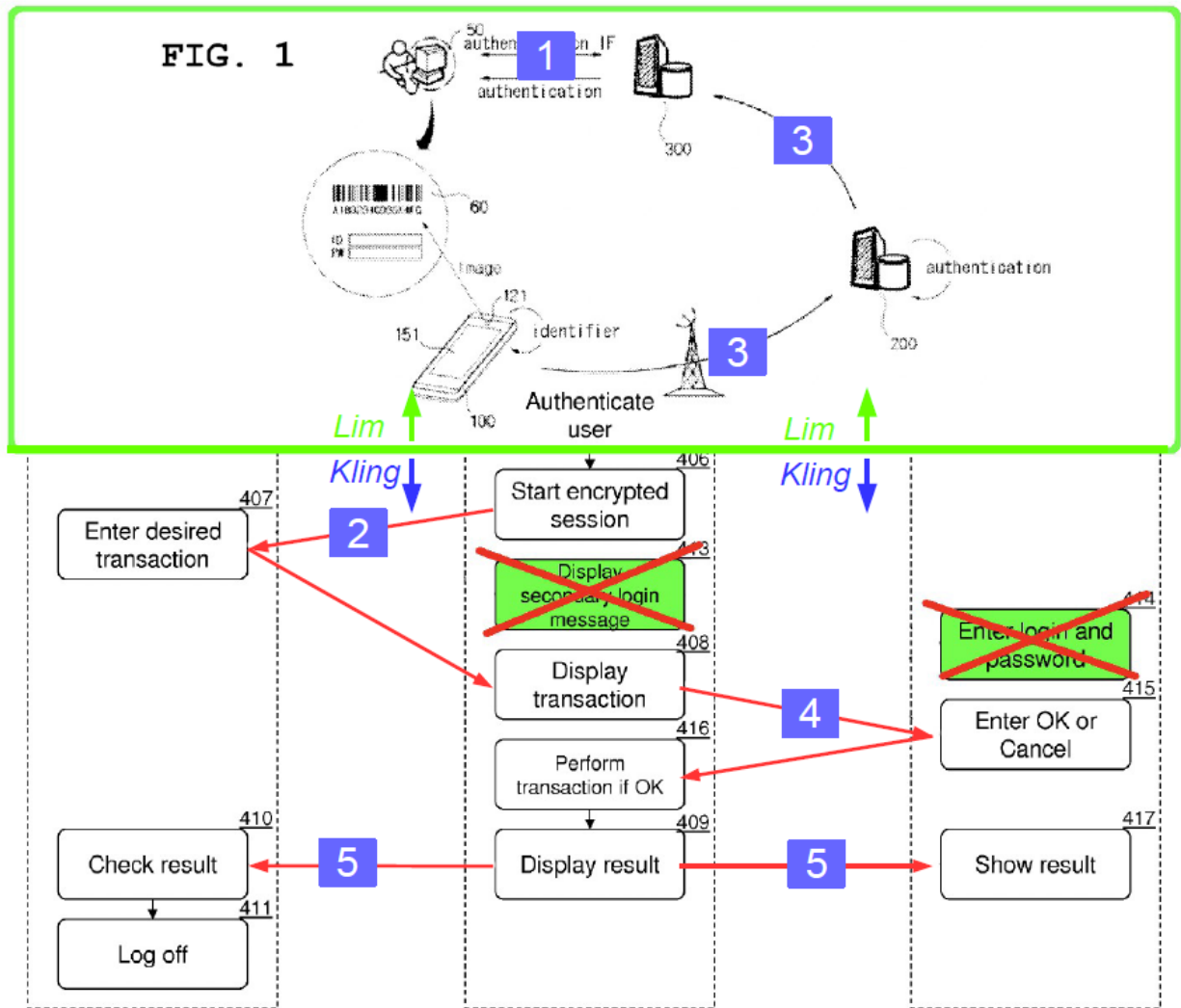
security” (Ex-1030 ¶[0010]) where “personal information ... stored in service servers are being divulged by the hacking of external intruders” (Ex-1030 ¶[0005]). A POSITA reading *Lim* understands that personal information such as bank information is less susceptible to hacking when it is not transmitted until after the user has logged in using two devices (the PC and the phone).

121. In addition, 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.

122. A POSITA would have a reasonable expectation of success in modifying *Kling* according to *Lim*’s teaching (i.e., to authenticate the user on the mobile device prior to starting the encrypted session) 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.

123. As an alternative example, the teachings of *Lim* would have motivated a POSITA to modify the process illustrated in Figure 4 of *Kling* to replace the login/authentication process of *Kling* with the login/authentication process of *Lim*, as illustrated below.



- 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

124. A POSITA would have been motivated to modify *Kling* to replace the login/authentication steps associated with both the user PC and the secondary mobile

phone with the two-device login/authentication process taught by *Lim* prior to starting an encrypted session.

125. *Kling* teaches to protect banking transactions from malware:

As consumer online transactions such as for electronic banking are becoming much more widespread so are the incidents of compromised accounts and associated losses. In particular, consumers are likely to use very insecure platforms such as PCs and mobile phones which are prone to malware attacks.

Ex. 1023, ¶ [0003].

126. Similarly, *Lim* teaches to protect banking transactions from malware—“even if the user terminal is attacked by a hacker or malware and therefore the identifier is stolen, it is not possible to perform any authentication related to a user using the identifier” (Ex. 1030, ¶ [0044]) . . . which protects transactions with “the website of a financial institution such as a bank” (Ex. 1030, ¶ [0024]). A POSITA would have understood malware was a known problem in computer network systems, particularly internet systems, at the time of the alleged invention. The universal motivations to protect against malware would have motivated a POSITA to combine security measures. Thus, a POSITA would have been motivated to modify *Kling* to authenticate the user via login on both the user PC and the secondary mobile phone, as taught by *Lim*. 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.

127. 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

[o]nce the success of the authentication has been notified by the authentication information processing module 250, 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].

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* would be successful in improving the overall security of *Kling* and preventing the types of malware attacks *Lim* discusses.

5. [26d] “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.”

128. *Kling* discloses this element. Specifically, *Kling* teaches to transmit distinct subsets of information to the PC and mobile device, if and only if, both “devices” are accessible by the bank server 401. In particular, *Kling* discloses to send bank web site pages to “enter desired transaction” 507 and “display transaction” 508, if and only if, the user has logged into the PC and the mobile device, respectively. Ex. 1023, Figure 2, [0014] (“the user would open a Web site 2020, in this example of a bank, [and be] prompted for a login and password 203, 204.”); Fig. 4, [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”) “***Upon receiving the user’s transaction request*** the bank server may decide, based on a set of rules to invoke a secondary authentication request 413.” Ex. 1023, [0017]. “Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC. ***Subsequently***, a secure session is established between the

bank server and the mobile device and the transaction is displayed for confirmation 408.” Ex. 1023, [0018].

129. *Kling* shows a flow chart for sending subsets of information “if and only if” the remote bank server 401 authenticates the user on the PC and the mobile device. Ex. 1023, Figure 4. The remote bank server 401 generates and sends a “display login screen” 403 so the user may “enter login and password” 404 on the PC. “If and only if” the remote bank server 401 has authenticated the user 405 on the PC, the remote bank server 401 “starts encrypted session” 406, generates and sends a web page to the PC for the user to “enter desired transaction” 407 via the PC. After the remote bank server 401 receives the “desired transaction,” the remote bank server 401 generates and sends a “display secondary login message” 413 to the mobile device for the user to “enter login and password” 414. “If and only if” the user is authenticated on the mobile device, then the remote bank server 401 generates and sends a “display transaction” 408 web page to the mobile device, and the user may “enter OK or cancel” 415 on the mobile device.

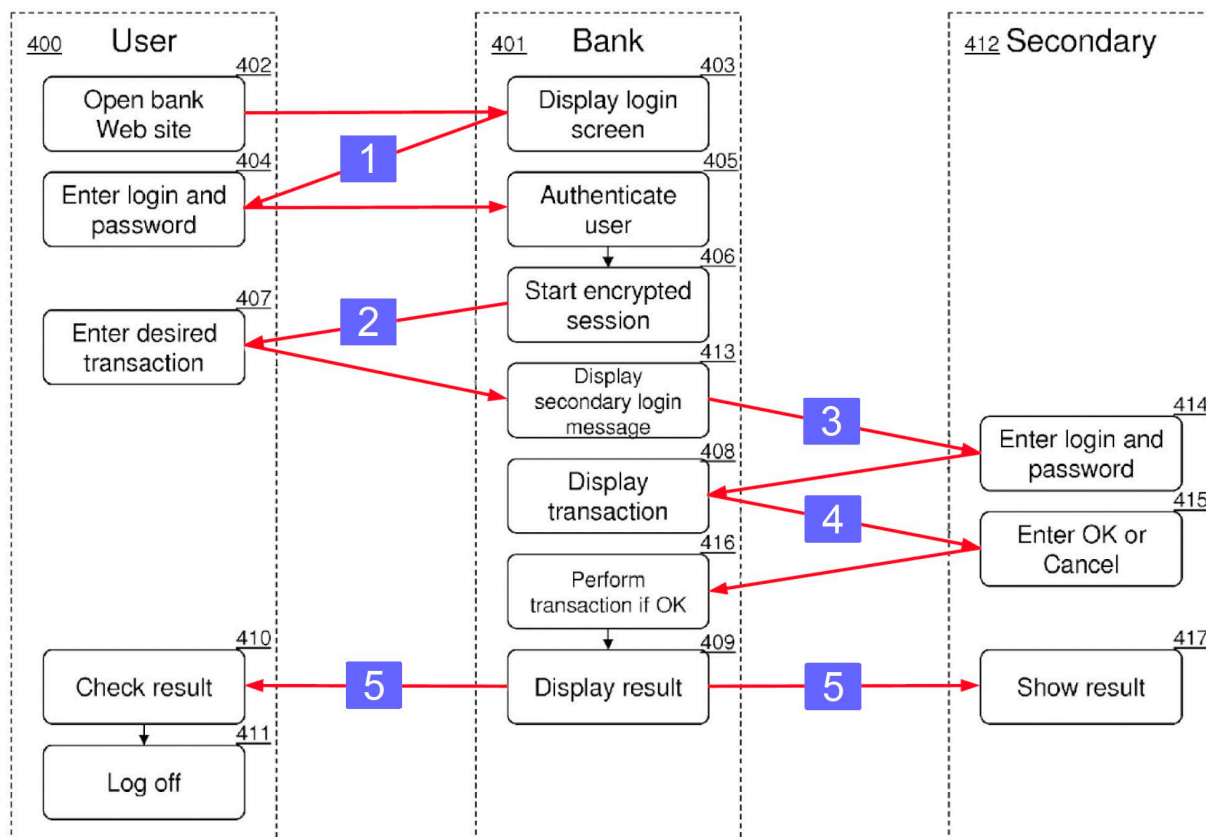


FIG. 4

- 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 page information

Ex. 1023, Figure 4 (revised and annotated).

130. Patent Owner argues *Kling* does not disclose the “if and only if” limitation. Although I disagree with this argument, it is my opinion this limitation would have been obvious in view of *Lim*. In particular, it would have been obvious to modify *Kling* to communicate bank transaction information “if and only if” both

devices are determined to be accessible by the server (i.e., the user is authenticated via logins on both the user PC and secondary mobile phone, as taught by *Lim*).

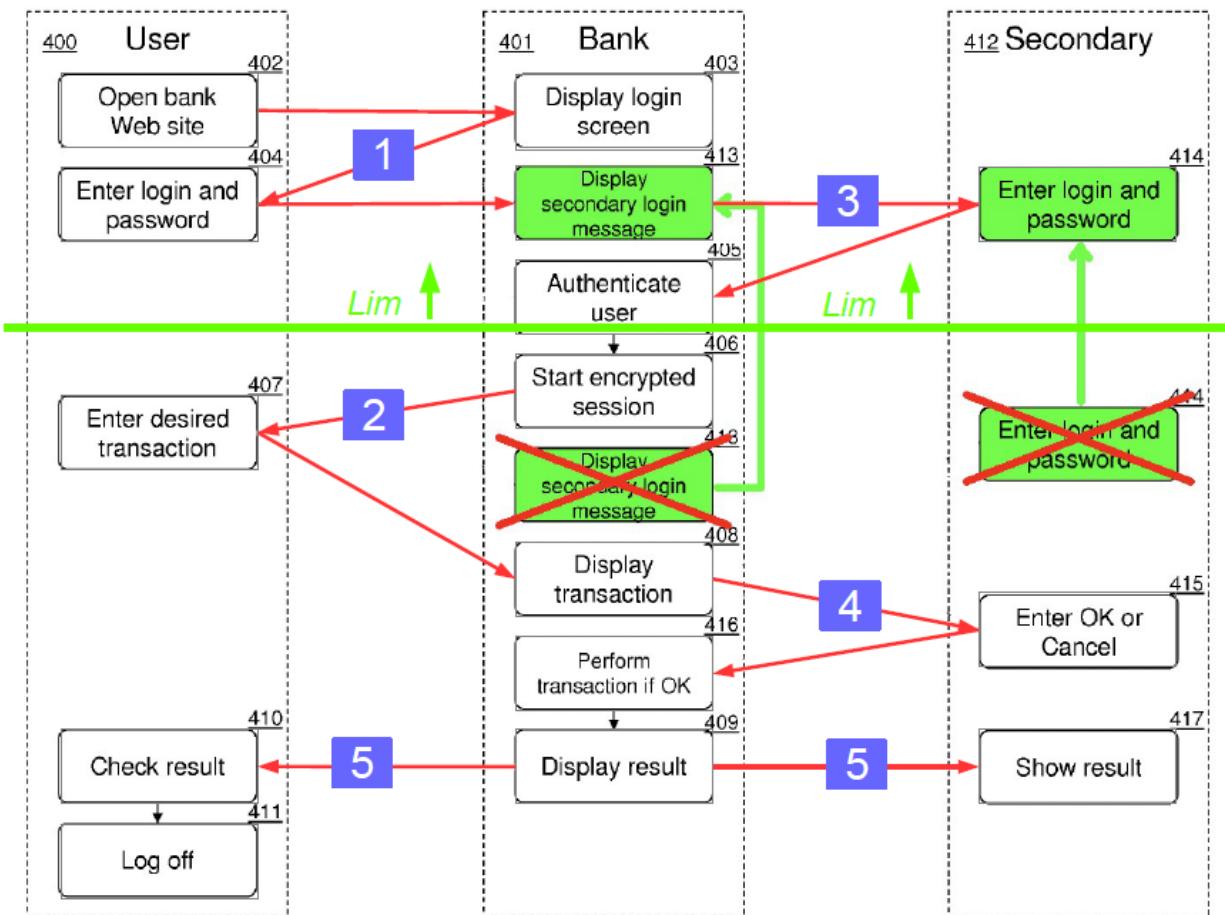


FIG. 4

- 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

131. *Lim* expressly teaches to transmit information “if and only if both the first and second devices are determined to be accessible by the server,” as claimed.

The authentication system 200 obtains authentication information from the mobile terminal 100 if the identifier information sent by the mobile terminal 100 is identical to the identifier information related to the identifier provided by the service server 300, and notifies the service server 300 of authentication results (the success of authentication or the failure of authentication) if pieces of authentication information are identical to each other. The service server 300 authenticates the user terminal 50 to which the identifier was issued based on the authentication results, and then determines whether login can be successful.

Ex. 1030, ¶ [0047].

Once the success of the authentication has been notified by the authentication information processing module 250, 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] (emphasis added).

132. Thus, *Lim* discloses the [26d] “if and only if” limitation.

133. For similar reasons to those discussed above for the previous limitation, it is my opinion that *Kling*’s and *Lim*’s goal of preventing malware breaches in banking applications would motivate a POSITA to implement the “if and only if” function in *Kling* and it is also my opinion that a POSITA would be successful in modifying *Kling* to require both the PC and the mobile device to be logged in and accessible prior to starting encrypted session 406 and sending the “display transaction” web site page (408/508) because *Kling* does not send that page until

after the user has been authenticated 405 via being logged in to each device, respectively.

134. A POSITA would have been motivated to modify *Kling* to “start encrypted session” 406 if and only if “authenticate user” 405 has been successful on both the user PC 400 and the secondary mobile phone. *Lim* teaches to move the *Kling* login steps associated with the secondary mobile phone (“Display secondary login message” 413 and “Enter login and password” 414) to coincide with the login steps associated with the user PC 400 (“Display login screen” 403 and “Enter login and password” 404). *Lim* expressly teaches to transmit bank transaction information after login on both devices.

Once the success of the authentication has been notified by the authentication information processing module 250, 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. 2030, ¶ [0077].

135. A POSITA would have been motivated to modify *Kling* to protect against malware. *Kling* teaches to protect banking transactions from malware—

As consumer online transactions such as for electronic banking are becoming much more widespread so are the incidents of compromised accounts and associated losses. In particular, consumers are likely to

use very insecure platforms such as PCs and mobile phones which are prone to malware attacks.

Ex. 1023, ¶ [0003].

136. Similarly, *Lim* teaches to protect banking transactions from malware—“even if the user terminal is attacked by a hacker or malware and therefore the identifier is stolen, it is not possible to perform any authentication related to a user using the identifier” (Ex. 1030, ¶ [0044]) . . . which protects transactions with “the website of a financial institution such as a bank” (Ex. 1030, ¶ [0024]). Thus, a POSITA would have been motivated to modify *Kling* to authenticate the user via login on both the user PC and the secondary mobile phone, as taught by *Lim*.

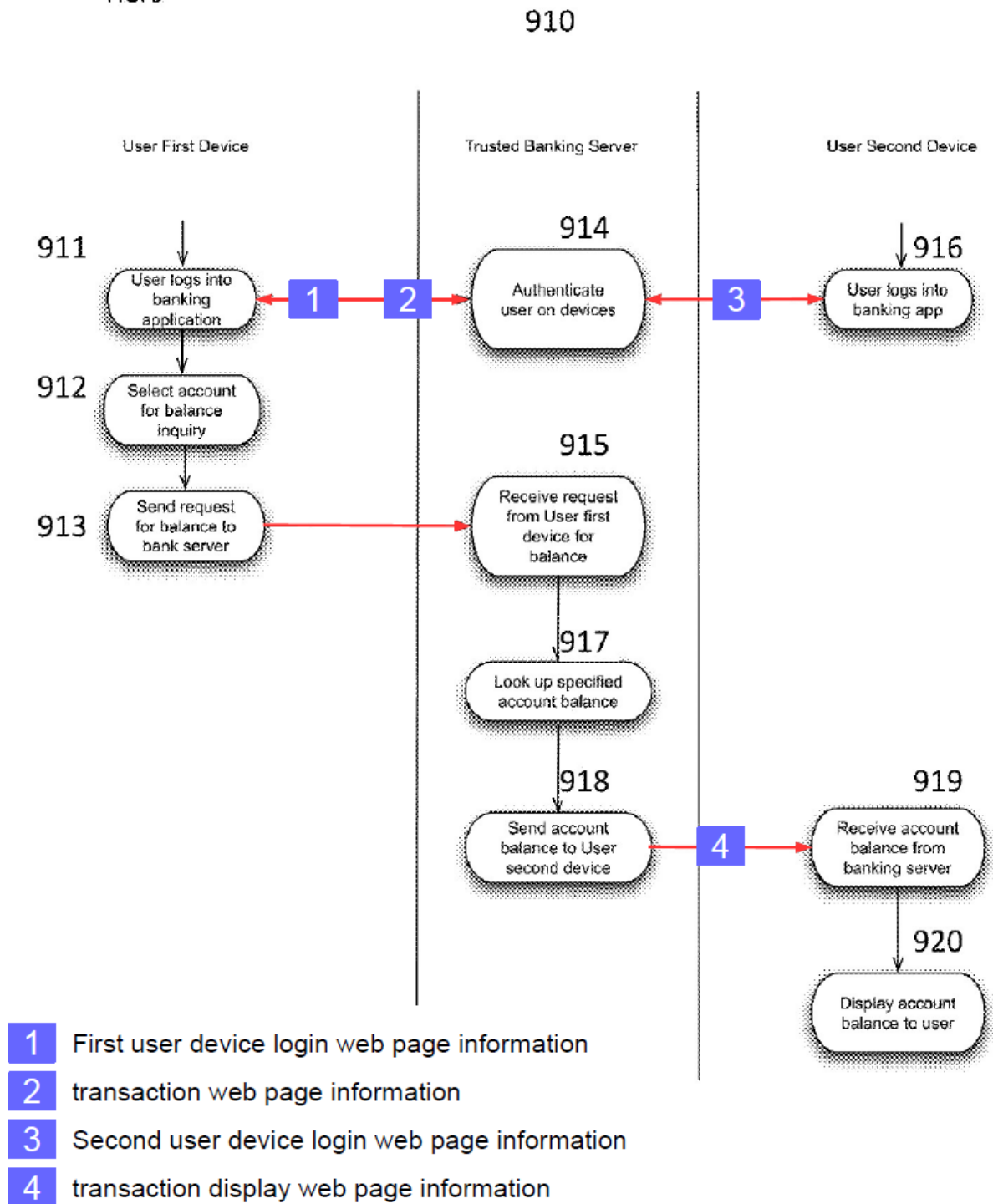
137. For the reasons discussed above for the previous limitation, a POSITA would have expected success in modifying the *Kling* Figure 4 process to “start encrypted session” 406 if and only if “authenticate user” 405 has been successful on both the user PC 400 and the secondary mobile phone.

138. Further, *Kling* is very similar to the '376 Patent “banking” example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent “banking” example meets this [26d] “if and only if” limitation where the “Trusted Banking Server” logs in the user on both a User First Device and a User Second Device, using different passwords, prior to sending subsets of information. Ex. 1001, Figures 8-9, 9:65-10:9.

As illustrated in FIG. 9, using a first device, a user logs into a banking application (911), selects an account for balance inquiry (912), and sends a request for a balance to a bank server (913). Using a second device, the user logs into a banking application (916). A banking server authenticates the user on the two devices (914). The banking server then receives a request from a user on the first device for a balance (915), looks up the specified account balance (917), sends the account balance to the user on the second device (918).

Ex. 1001, 9:65-10:7, Figure 9.

FIG. 9



Ex. 1001, Figure 9, 9:65-10:9 (revised and annotated).

139. Similarly, *Kling* as modified in view of *Lim*, meets this [26d] “if and only if” limitation where the “bank server” 401 logs in the user on both a user PC and a user mobile device, using different passwords, and “if and only if” the user is authenticated sends subsets of information.

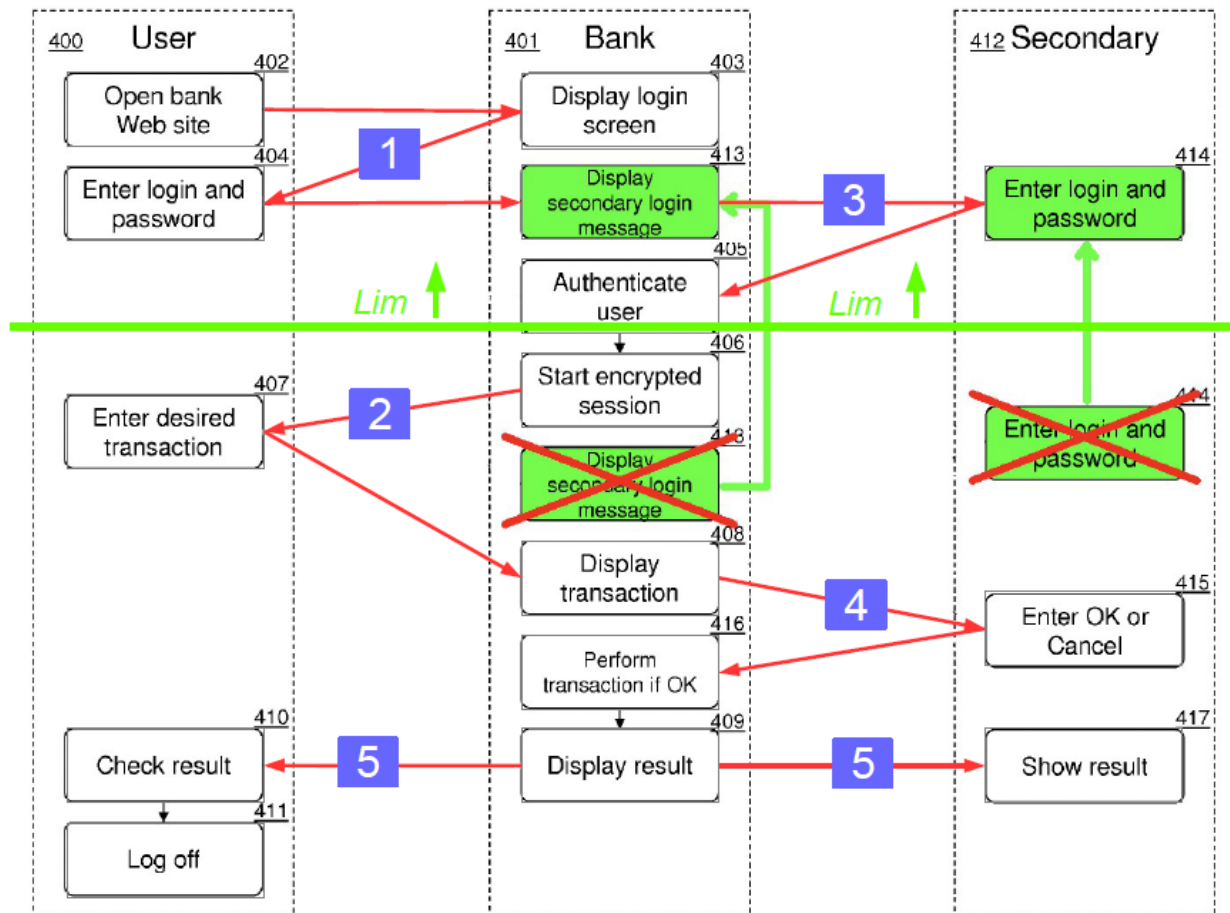


FIG. 4

- 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

D. Revised Substitute Claim 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.”

140. *Kling* and *Lim* disclose this claim. This element requires a portion of the first subset of information that was transmitted to the first device to also be transmitted to the second device under the condition that satisfies the “if and only if” requirement in revised amended claim 26.

141. *Kling* discloses the user may open a bank web site via both the user’s PC and the user’s mobile device, which prompts for a username and password on both a user’s PC and a user’s mobile device. “Typically, the user would open a Web site 202, in this example a bank. After being prompted for a login and password 203, 204 a presumably secure transaction session is opened with the remote server 205, 206.” Ex 1023, [0014]. Similarly, “the mobile device may open up a Web browser or invoke a specialized mobile banking app upon receipt of the server notification.” Ex 1023, [0017]. 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,” as claimed. The results web page information [Arrow #5] corresponds to the “at least a portion of the first subset of information,” as claimed. Further, *Kling* teaches that “If the user confirmed the transaction, the server will process it 416 and generate a result page 409, which is displayed on the user’s PC and mobile device 417.” Ex. 1023, [0018]. The “result page 409” (results

web page information [Arrow #5]) generated by the banking application and displayed in the web browser of both the PC and the mobile device also corresponds to the “transmitting at least a portion of the first subset of the information to the second device.”

142. For the “only if both the first and second devices are determined to be accessible by the server” limitation, it is my opinion a POSITA would read this limitation as effectively a subset of the “if and only if” requirement of claim 26 because the condition is essentially the same (accessibility of both devices). Thus, it is my opinion that *Kling* and *Lim* render 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.

E. Revised Substitute Claim 28 — “The method of claim 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”

143. Although I disagree that Patent Owner has identified sufficient written description support for the new term “the sensitive information is only shared with the second device” (see discussion above), I evaluate the patentability of the revised substitute claims based on Patent Owner’s apparent reliance on the disclosure of not transmitting sensitive information to a device other than the second device while the information is sensitive. *Kling* discloses this claim.

144. *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] generated by the bank server 401 to "start encrypted session" 406 and invite the user to "enter desired transaction" 407 corresponds to the first subset of information, which comprises "non-sensitive information" as claimed. A POSITA understands that after logging into a system such as *Kling*'s banking application, the application would be expected to provide generic information about banking, banking offers available to the public, and general information about the bank that it would share with users and non-users of the bank (e.g., location of the corporate headquarters, security of the bank, that the bank is insured, offering of services, bank name, bank, logo, etc.). A POSITA would find it obvious to include these types of non-sensitive information in the web page information accompanying *Kling*'s "enter desired transaction" web page. It would be obvious to include other non-sensitive web page information such as the page layout and navigation features.

145. Further, the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to "display transaction" 408 so the user may "enter OK or Cancel" 415 corresponds to the second subset of information, which comprises "sensitive information," as claimed. The invitation enabling the approval of a transfer of funds and providing the means to do so, such as transaction identifiers

or cookies, (the “OK” response) is clearly sensitive because it provides the ability to finally perform a critical transaction such as transferring money to an external account.

146. *Kling* teaches the transaction confirmation web page information [Arrow #4] is only shared with the user’s mobile device to prevent malware from capturing and modifying the desired transaction. Ex. 1023, Figure 5, [0019]. By teaching to keep the transaction confirmation web page information [Arrow #4] from the malware, *Kling* clearly teaches the transaction confirmation web page information [Arrow #4] is “sensitive information” that is “only shared with the second device,” as claimed.

147. Patent Owner incorrectly states, “Petitioner identifies ‘enter OK or Cancel’ as the ‘sensitive information,’ and argues “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.” RMTA at 11. I disagree.

148. The Board gave “sensitive information” its ordinary and customary meaning as would have been understood by one of ordinary skill in the art. *See e.g.*, Ex. 3002, Margaret Rouse, *Sensitive Information*, TECHOPEDIA, <http://www.techopedia.com/definition/25260/sensitive-information#> (last updated Sept. 26, 2012)(last visited Mar. 6 2024) (“Sensitive information refers to privileged or proprietary information that only certain people are allowed to see and that is

therefore not accessible to everyone.”). PG at 20. As noted above, Petitioner has identified the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to “display transaction” 408 as the “second subset of information.” Whereas the words “OK or Cancel” may not be sensitive as such, the fact that they are active web buttons which include the information necessary to activate a financial transaction clearly is sensitive. Thus, the sensitive information provided to the second device comprises the specific transaction information and the information required to effect the transaction itself (e.g., the HTML information that informs the device how to effect the sensitive transaction.) The transaction confirmation web page information [Arrow #4] satisfies the Board’s construction because it is not accessible to the user PC 400 and it is “privileged information that only certain people [i.e., the user] are allowed to see and that is therefore not accessible to everyone” (i.e., not accessible to anyone other than the person using the mobile device). Contrary to Patent Owner’s argument, disclosure of the transaction confirmation web page information [Arrow #4] to the user PC 400 would be harmful because a malware infected device would be able to use it to confirm the transaction.

F. Revised Substitute Claim 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”

149. *Kling* discloses this claim. *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]. As noted above, 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 corresponds to the first subset of information, which comprises “non-sensitive information” as claimed. Further, the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to “display transaction” 408 so the user may “enter OK or Cancel” 415 corresponds to the second subset of information, which comprises “sensitive information,” as claimed.

150. *Kling* teaches the transaction confirmation web page information [Arrow #4] is transmitted to the user’s mobile device to prevent malware from capturing and modifying the “desired transaction.” Ex. 1023, Figure 5, [0019]. By teaching to keep the transaction confirmation web page information [Arrow #4] from the malware, *Kling* clearly teaches the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to “display transaction” 408 so the user may “enter OK or Cancel” 415 via 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’s more sensitive because it is the information that is required to authorize a transaction such as transferring money to another account.

G. Revised Substitute Claim 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 on the second device that the connectivity has been disrupted.”

151. *Kling* discloses this claim. *Kling* discloses the second device (mobile phone) utilizes a web browser access the bank server. Ex. 1023, ¶ [0005] (“In one embodiment, no special software is required on the client devices at all, a regular Web browser is sufficient for this purpose.”). It is my opinion that a POSITA would understand that web browsers utilize the HTTP protocol, and that the web browser executing on the mobile phone (second device) would determine if connectivity between the server had been disrupted when it did not receive a response to an HTTP request it sent to the game server. After determining the connection has been disrupted, the browser would provide a notification on the mobile phone’s display (second device), for example, an HTTP status code “503 Service Unavailable.”

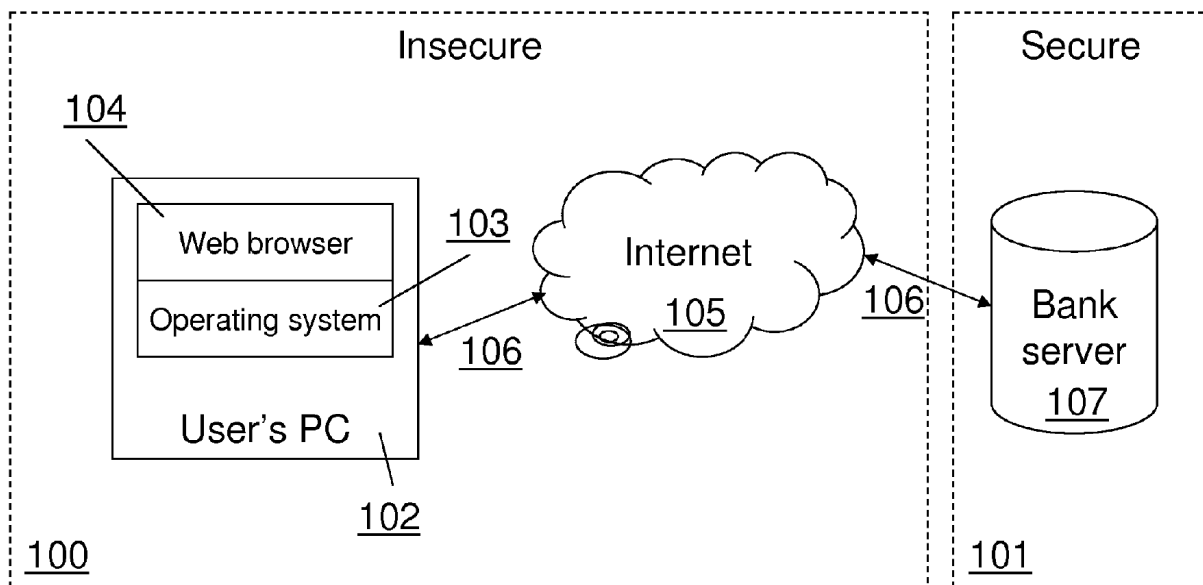
152. Further, *Gumbula* shows a POSITA has general knowledge of determining if a client-server connection is disrupted and, if so, providing a notification on the client device. *Gumbula* shows this knowledge in the context of

an HTTP connection, which is used by *Kling*. Ex-1011, Abstract (“Heartbeat messages are exchanged between the chat client and the server at predetermined time intervals. When a failure to receive a heartbeat message for longer than one of the predetermined time intervals, then a lost connection message is provided to at least one of the server and client.”), 1:56-60 (“conventional solutions available [in 2005 did] not transparently recover a lost Hyper Text Transmission Protocol (HTTP) connection between the server and the client, nor notify the status of the connection to the parties involved.”), 4:44-49 (“If either client 12 or the server component 14 does not see a heartbeat message during the check interval then the client 12 displays the message ‘Lost connection to the server, retrying...’ and the server component 14 sends a message to the agent 20 ‘Client has lost connection to the server, retrying...’.”).

153. Because *Kling* discloses an HTML-based banking system that is accessed by web browsers on both the first and second devices, the HTTP error notification is (1) necessarily present in or (2) the natural result of *Kling*’s web-browser-based banking application.

H. Revised Substitute Claim 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.”

154. *Kling* discloses this claim. In particular, *Kling* discloses, “[d]ue to the fact that PCs and mobile devices typically use different Web browsers, operating systems and communication channels the overall security of this two-factor-authentication is substantially higher than the original single factor authentication performed on a PC.” Ex. 1023, [0007].



Ex. 1023, Figure 1. “The secondary authentication request may be sent to a mobile device such as a cell phone that the user has previously registered with the bank server. Such a request can be sent by various means such as Internal ‘push’ data or SMS.” Ex. 1023, [0017]. Thus, *Kling* expressly teaches transmitting a first subset of the information (transaction web page information [Arrow #2] for “enter desired

transaction” 407) to the first device (PC) from the server (bank server 401) and transmitting a second subset of the information (transaction confirmation web page information [Arrow #4] for “display transaction” 408) to the second device (mobile device) from the server (bank server 401) are executed over independent electronic communications networks (Internet and cellular). Notably, a POSITA understands there is a distinction between a cellular network and a TCP/IP-based network (the Internet)—i.e., independent electronic communication networks.

155. It is my opinion a POSITA would understand Internet and cellular are independent electronic communications networks. Indeed, even the '376 Patent recognizes that cellular and the Internet are independent electronic communications networks: “Ethernet cable or wirelessly via WiFi or via some combination of wired and wireless connections. The second device may communicate with the central server via any one of multiple mechanisms. For example, the central server may utilize text messages via SMS to communicate with the second device. Or, the user can connect the second device to the Internet either via the cellular network’s Internet service such as a 3G or 4G (e.g., LTE) network or similar networks of the cellular provider, or using WiFi.” Ex. 1001, 11:38-46.

156. To the extent Patent Owner argues *Kling* does not expressly disclose “independent electronic communications networks,” it is my opinion this limitation would have been obvious in view of the POSITA’s general knowledge. A POSITA

would have understood that a cellular network is at least partially independent of the Internet, which is a TCP/IP-based network. A POSITA would understand that *Kling*'s disclosure of a mobile device or cellphone would teach that its transmissions would be across a cellular network. *Kling*'s disclosure of a user logging into a personal computer would disclose to a POSITA a TCP/IP-based network (Internet), which is independent of a cellular communication network.

157. In view of *Kling*'s disclosure that transmission may be via Internet and cellular (Ex. 1023, Figure 1, [0007], [0017]) and the '376 Patent's recognition that these are independent networks (Ex. 1001, 11:38-46), a POSITA would understand those to be "independent electronic communications networks," as claimed.

I. Revised Substitute Claim 32 — "The method of claim 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"

158. As discussed above, the scope of "the information displayed on the respective devices" is unclear. As best understood, *Kling* discloses this claim.

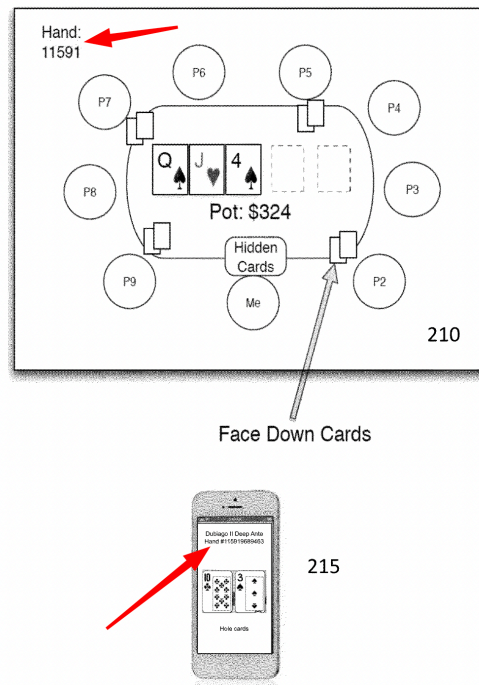
159. First, *Kling* discloses a user "[e]nter[s] desired transaction 407" (Ex. 1023, Fig. 4), which entails displaying details of the transaction. In *Kling*'s example of "transfer[ing] a certain sum of money to another account" (Ex. 1023, ¶ [0014]), the user's PC would display the source account, the amount, and the destination account. That same information would be displayed on the user's mobile phone

based on the “[d]isplay transaction 408” step in Figure 4. A POSITA would understand this information to be “a graphical identifier on the first device” (in step 407) and “a corresponding graphical indicator on the second device” (in step 408) that “indicat[e] a link between the information displayed on the respective devices.” The very purpose of repeating the same graphical information is to link the transaction information displayed on the mobile phone with the transaction initiated by on the user’s PC so the user can confirm the transaction (“Enter OK or Cancel 415”). Ex. 1023, ¶¶ [0017]-[0018].

160. Alternatively, *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 in the funds transfer example. A POSITA would understand this information to be “a graphical identifier on the first device” (in step 410) and “a corresponding graphical indicator on the second device” (in step 417) that “indicat[e] a link between the information displayed on the respective devices.” The very purpose of displaying the same graphical information on both devices is to indicate a link between the two result pages so that the user can verify that the transfer was performed successfully. Ex. 1023, ¶ [0018].

161. Based on the ’376 Patent, a POSITA understands that text on these pages (source account, amount, destination account) are “graphical identifiers” or “graphical indicators.” Indeed, “FIG. 2 illustrates an example ... whereby an

identifier links two separate computing devices” (Ex. 1001, 2:5-6), and Figure 2 includes a text-based identifier (“**Hand 11591**” on the first device and “**Hand #115919689463**” on the second, mobile device):



Ex. 1023, Fig. 2. Thus, the '376 Patent teaches the graphical identifier and graphical indicator can be text.

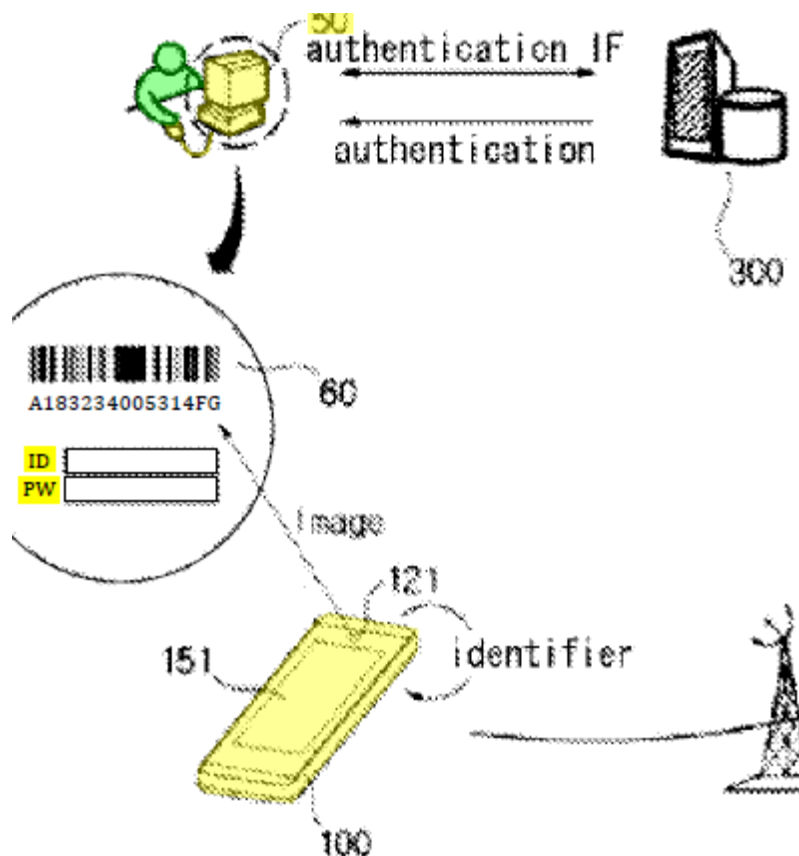
162. In addition, the '376 Patent specification uses the term “graphical” only once, explaining “The systems and methods described herein can be implemented in a computer system that includes ... a front-end component, such as a client computer having a **graphical user interface** or an Internet browser, or any combination of them.” Ex. 1001, 14:38-44 (emphasis added). A POSITA understands that

“graphical” refers to something (e.g., a user interface) displayed on a screen such as a computer monitor or phone screen—including text.

J. Revised Substitute Claim 34 — “The method of claim 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”

163. *Kling* and *Lim* disclose this claim. *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.

164. “Referring to FIG. 1, in an authentication method according to the present invention, when the user terminal 50 connects with the service server 300 and performs authentication, for example, performs login, the service server 300 provides an authentication interface including an identifier to the user terminal 50.” Ex. 1030, [0028].



Ex. 1030, Figure 1 (highlighted).

165. “Once the authentication interface including the identifier 60 has been displayed on the monitor of the user terminal 50, a user captures the identifier 60 using the mobile terminal 100.” Ex. 1030, [0033]. By requiring the user to “send the captured identifier 60 to the authentication system 200,” it confirms the displays of the user terminal 50 and the mobile terminal 100 are being viewed exclusively by the same user. Thus, *Kling* in view of *Lim* discloses the [34] “exclusive viewing” limitation. As discussed above for claim 26, the teachings of *Lim* would have motivated a POSITA to modify the process illustrated in Figure 4 of *Kling* to replace the login process of *Kling* with the login process of *Lim* (as depicted below).

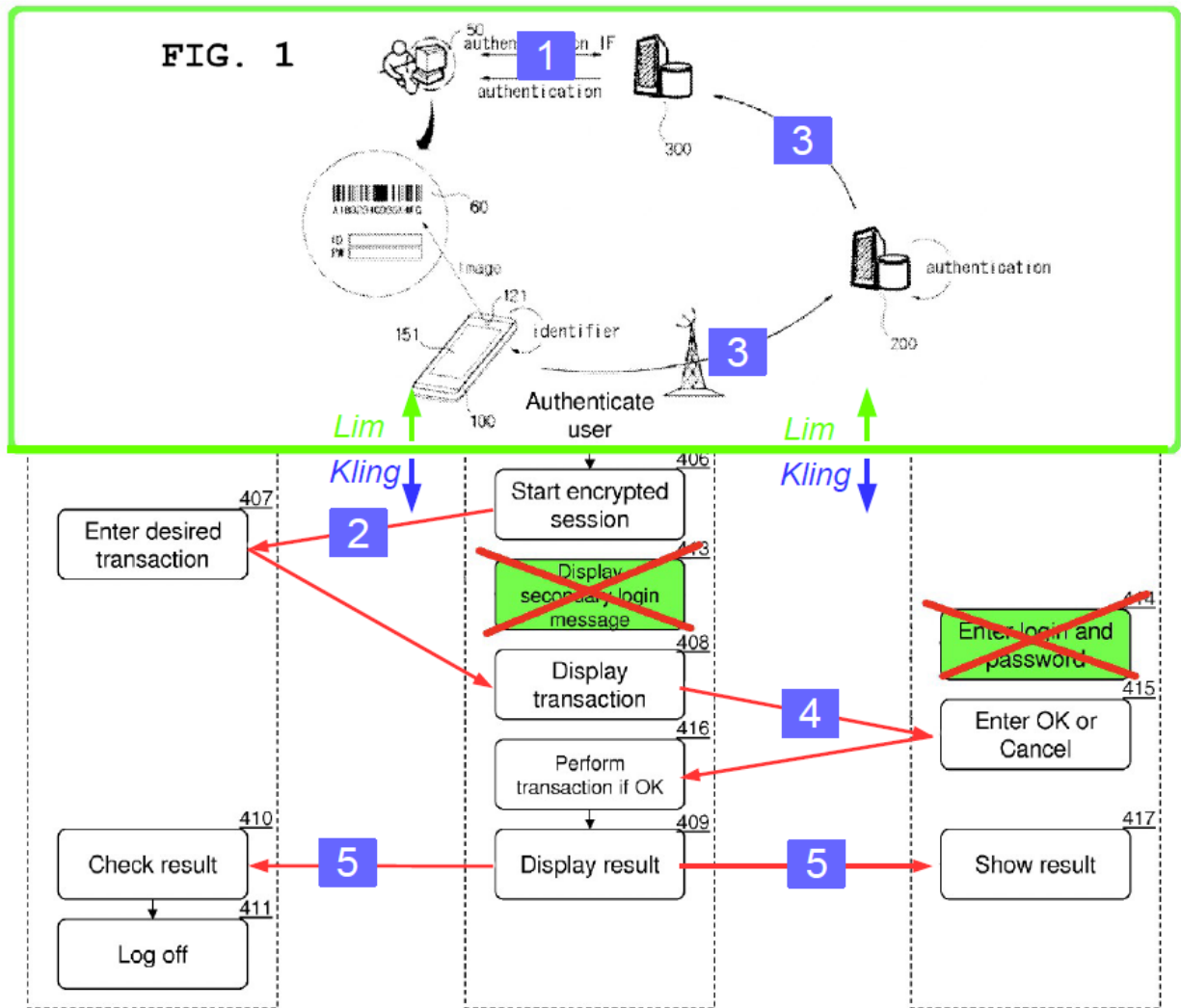


FIG. 4

- 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

- K. Revised Substitute Claim 35 — “The method of claim 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.”**

166. As discussed above, the scope of “the information displayed on the respective devices” is unclear. As best understood, *Kling* discloses this claim.

167. In *Kling*, the first and second subsets do not comprise a two factor authentication code. As discussed above for claims 26-27, the first subset of information includes the transaction web page information [Arrow #2] and the results web page information [Arrow #5] generated by the bank server. This information does not comprise a two factor authentication code. Also as discussed above for claims 26-27, the second subset of information includes the transaction display web page information [Arrow #4], which is also not a two factor authentication code. *Kling* does not describe two factor authentication. Accordingly, neither the first subset of information nor the second subset of information comprise a two factor authentication code.

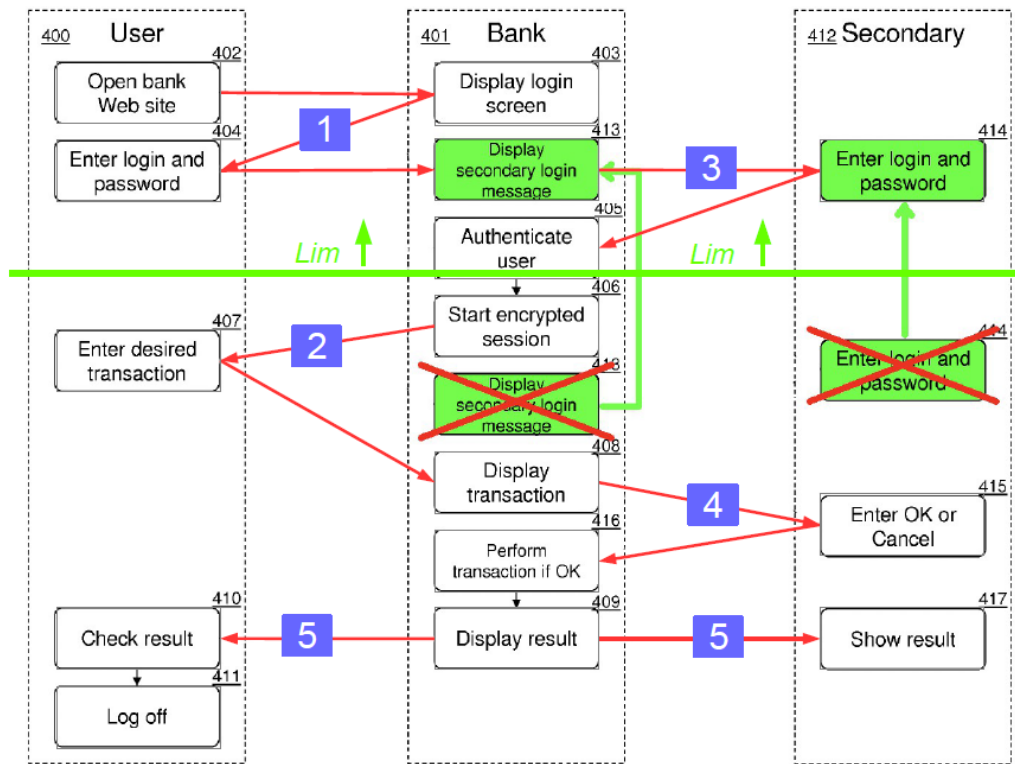


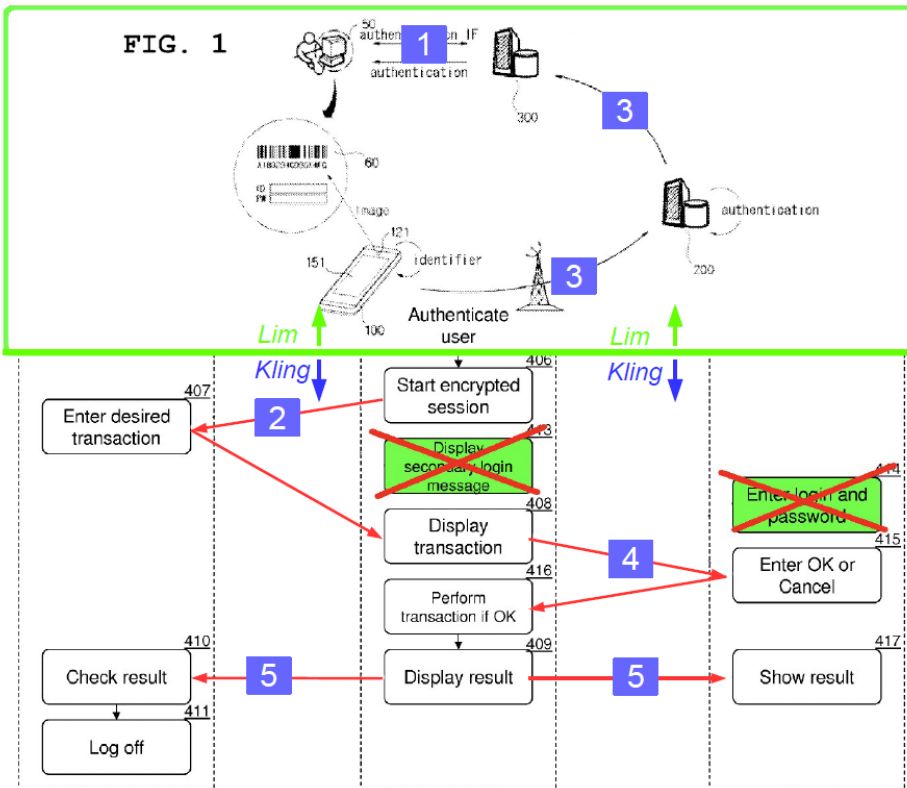
FIG. 4

- 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

168. Accordingly, in *Kling* alone or as modified by *Lim* (as shown in the annotated figure above), neither the first subset of information nor the second subset of information comprise a two factor authentication code.

169. The same is true of the other *Kling/Lim* combination where *Lim*'s authentication scheme replaces *Kling*'s authentication (annotated figure below). As discussed above for claims 26-27, the first subset of information in this combination includes the transaction web page information [Arrow #2] and the results web page

information [Arrow #5] generated by the bank server. This information does not comprise a two factor authentication code. Also as discussed above for claims 26-27, the second subset of information includes the transaction display web page information [Arrow #4], which is also not a two factor authentication code.



170. Revised substitute claim 35 includes the same limitation found in revised substitute claim 32 (graphical identifier on first device and graphical

indicator on second device indicating a link...). My analysis for revised substitute claim 32 applies equally here.

L. Revised Substitute Claim 39 — “The method of claim 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.”

171. *Kling* discloses this claim. *Kling* discloses “the bank server may decide, based on a set of rules to invoke a secondary authentication request 413. Such rules could take into account various factors such as the transaction amount and type, the user’s security history, the type of Web browser used and the like.” Ex. 1023, ¶ [0017]. A POSITA understands that a rule based on transaction amount (e.g., specifying a minimum transaction that requires secondary confirmation for the banking transaction) would use a parameter that is the threshold amount. A POSITA understands that this parameter would be electronically stored in *Kling*’s bank server. This parameter would indicate whether subsets of the information are to be divided between two or more devices. For example, if the amount of the transaction is below the minimum threshold, the subsets would not be divided.

I note that my opinion related to revised substitute claim 39 is guided by, and is consistent with, Patent Owner’s apparent understanding of this claim. In particular, I am informed that Patent Owner provided infringement contentions in the related district court litigation and alleges infringement of original claim 23 (for which revised substitute claim 39 is a substitute) because “The Kahoot! server must

have information that indicates how to communicate with the shared computer and how many mobile devices are involved in the quiz. That information is a parameter indicating whether subsets of the information are to be divided between two or more devices.” Ex. 1014-16.

M. Revised Substitute Claim 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.”

172. *Kling* discloses this claim. *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] generated by the bank server 401 to “start encrypted session” 406 and invite the user to “enter desired transaction” 407 corresponds to the first subset of information, which derives from functions within the banking application of the banking server. Further, the transaction confirmation web page information [Arrow #4] generated by the bank server 401 to “display transaction” 408 so the user may “enter OK or Cancel” 415 corresponds to the second subset of information, which also derives from functions within the banking application of the banking server. Patent Owner did not contend otherwise.

N. Independent Revised Substitute Claim 41

- 1. [41Preamble] “A system for protecting information by transmitting information to multiple electronic devices, the system comprising:”**

173. To the extent the preamble is limiting, *Kling* and *Lim* discloses this element.

174. *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].

175. Further, *Kling* is very similar to the '376 Patent “banking” example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent “banking” example meets the [26Preamble] where it discloses a bank server 813 transmitting information to a user's computer 812 and a user's smart phone 815. Ex. 1001, Figure 8, 7:63-8:9. Similarly, *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]. Thus, *Kling* discloses this element.

176. *Lim*'s system

authenticates a user using identifiers and authentication information provided and displayed by the mobile terminal and the service server to and on the user terminal, in conjunction with each other. Accordingly, unless an external intruder collects information necessary for authentication from the mobile terminal, the service server, and the user terminal in the same time span, the external intruder cannot perform authentication in place of a user. The present invention can be used to process authentication in portal sites, websites of financial institutions such as banks, personal blogs, homepages, and a variety of other websites using the Internet.

Ex. 1030, ¶ [87].

177. As explained, *Lim* sends information to both a user terminal and a mobile terminal. Thus, *Lim* discloses this element.

2. **[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”**

178. *Kling* discloses this element. *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.”

179. When *Kling* published in 2012, persons of skill in the art knew that a website includes web page information stored at the server. Thus, where *Kling* discloses “a Web site 202, in this example of a bank,” Ex. 1023, [0014], persons of skill in the art understood the web site provides a set of sufficiently specific banking information to allow the user to enter the specific transaction the user desires to engage in.

180. To the extent Patent Owner argues *Kling* does not expressly disclose “storage” of information at the server, it is my opinion this limitation would have been obvious in view of the POSITA’s general knowledge. For example, a POSITA

would understand that servers such as the *Kling* 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, such as PCs and mobile phones.

181. Evidence of the POSITA's general knowledge that servers store information the server ultimately transmits to client devices is found at least in U.S. Pub. No. 2014/0121015 to Massing et al. ("*Massing*") (Ex. 1017), as explained in my first declaration. Ex. 1002, ¶ 62.

182. *Kling* is very similar to the '376 Patent "banking" example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent "banking" example meets this [41a] "electronic data store" limitation where a "banking application" includes a "bank Web site" communicates from the server (Ex. 1001, Figure 8, 7:63-8:9). Similarly, *Kling* discloses a bank server 401 with a web site banking application. Ex. 1023, Fig. 4, ¶¶ [0017]-[0018]. Thus, *Kling* discloses this element.

183. For "wherein the first and second subsets of information are generated by the same application at the server and are specific to that application" of [41a], to the extent this element is understandable, *Kling* discloses this element. *Kling* discloses distinct subsets of information specific to "the Web site 202, in this example of a bank." Ex. 1023, [0014]. In particular, *Kling* discloses,

[a]fter being prompted for a login and password 203, 204 a presumably secure transaction session is opened with the remote server 205, 206. In this session the user may enter an online banking transaction 207, for

example to transfer a certain sum of money to another account” via a web page generated on the user’s PC.

Ex. 1023, ¶ [0014] & Figure 2; Figure 4, ¶ [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”); Figure 5, ¶ [0019] (“The initial login process 502-507 remains the same as previously described.”).

184. Thereafter,

typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC. Subsequently, a secure session is established between the bank server and the mobile device and the transaction is displayed for confirmation 408. The user can chose to confirm or cancel the request 415 which will terminate the secondary session.

Ex. 1023, ¶ [0018].

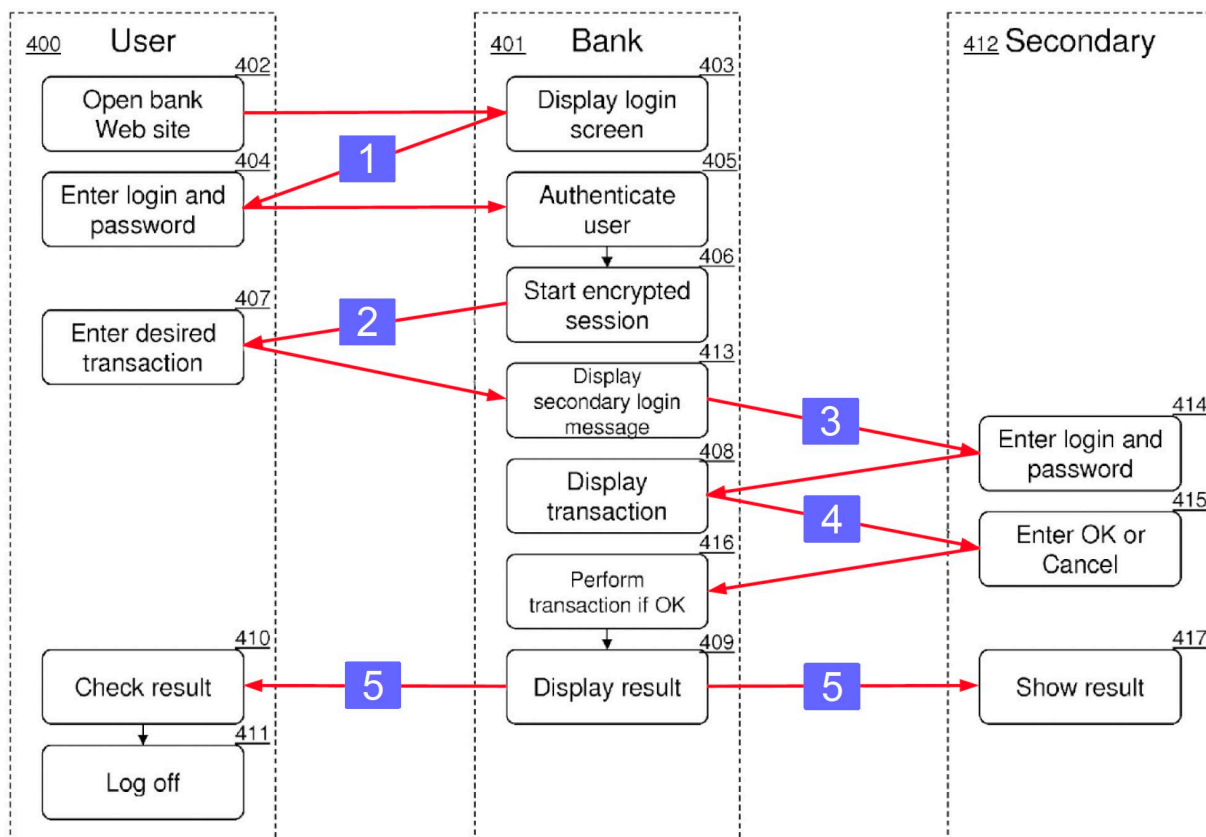


FIG. 4

- 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 page information

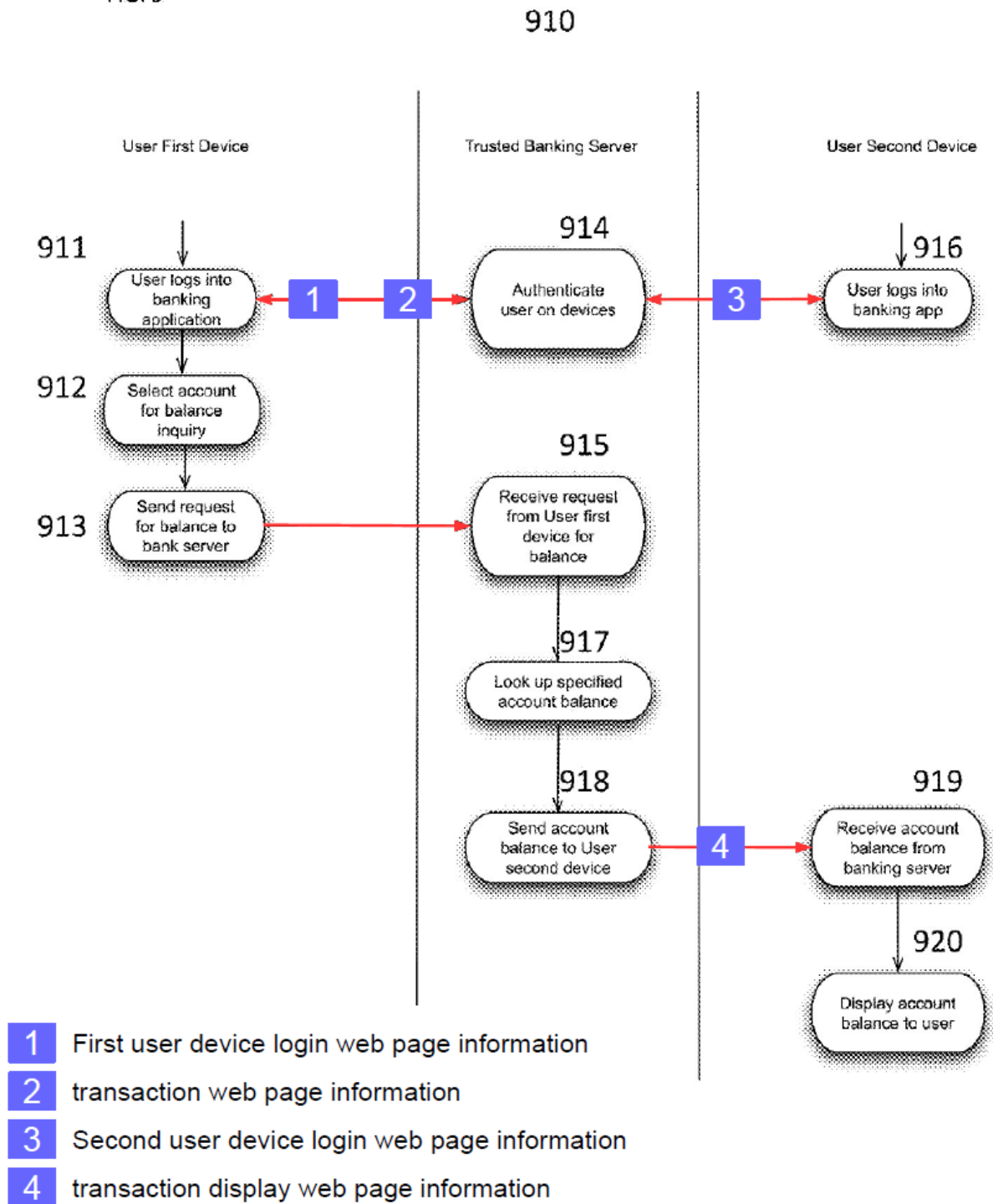
Ex. 1023, Figure 4 (revised and annotated).

185. First, the transaction web page information [Arrow #2] sent to the user's PC inviting the user to "enter an online banking 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 invite 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.

186. *Kling* is very similar to the '376 Patent “banking” example. Ex. 1001, Figures 8-9, 7:63-10:9. The '376 Patent “banking” example meets element 41b’s “subsets of information generated by the same application . . .” limitation where the transaction web page information [Arrow #2] sent to the user’s computer inviting the user to “transfer funds or check balance” is “a first subset of information” generated by the banking application at the bank server 813 and communicated to the user’s computer 812. The transaction display web page information [Arrow #4] sent to the user’s smartphone inviting the user to “transfer amount and transfer to:” is a “second subset of information” generated by the banking application at the bank server 813 and communicated to the user’s smartphone 815. Ex. 1001, Figure 8, 7:63-8:9. Further, Figure 9 shows the transaction web page information [Arrow #2] is “a first subset of information” generated by the “Trusted Banking Server” and communicated to the “User First Device” and the transaction display web page information [Arrow #4] is a “second subset of information” generated by the “Trusted Banking Server” and communicated to the “User’s Second Device.” Ex. 1001, Figure 8, 7:63-8:9.

FIG. 9



Ex. 1001, Fig. 9 (revised and annotated), 9:65-10:9.

187. Similarly, *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.

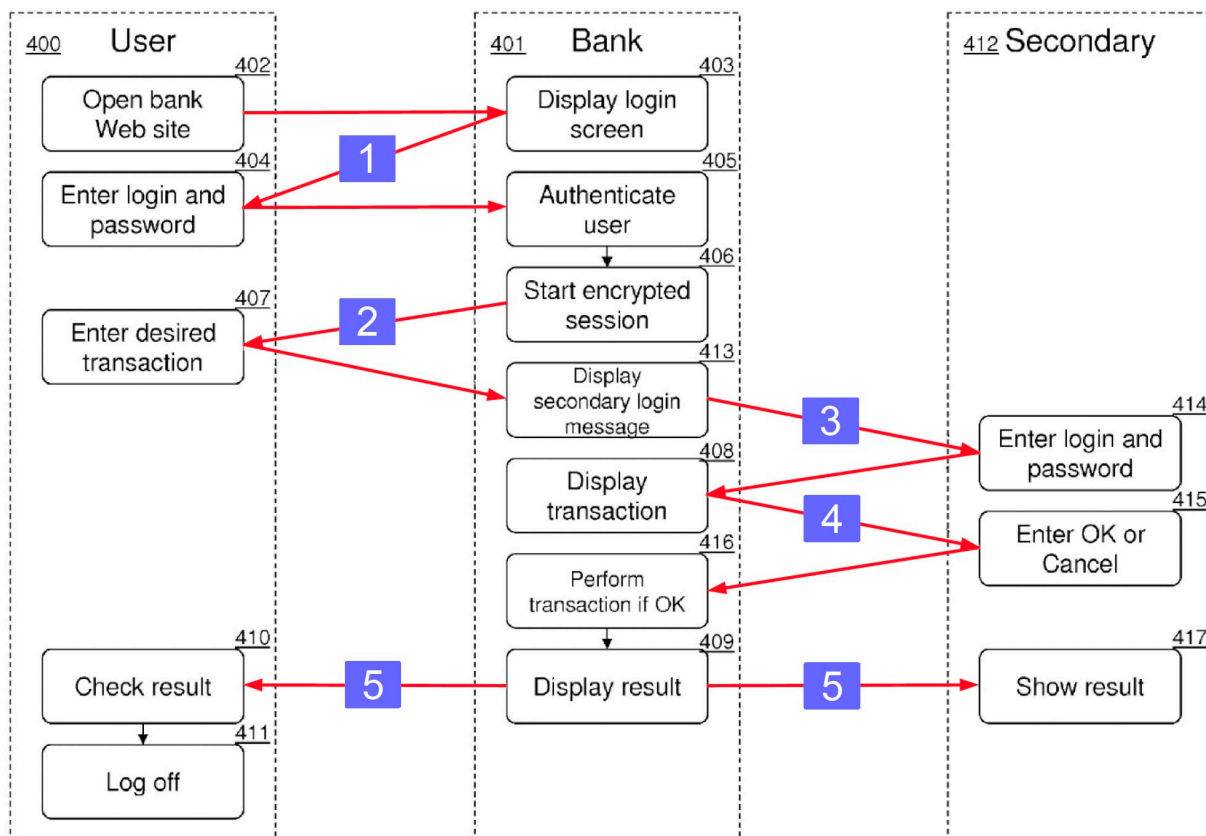


FIG. 4

- 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 page information

Ex. 1023, Figure 4, [0017]-[0018]. Thus, *Kling* discloses this element.

3. [41b] “a processor device programmed for:”

188. *Kling* and *Lim* disclose this element. *Kling* discloses a remote Banking server 107, 201, 301, 401, and 501, which a POSITA understands has a processor that is programmed. *Lim* discloses a banking website server 300, which a POSITA understands has a processor that is programmed.

4. [41c] “identifying a first subset of the information and identifying a second subset of the information;”

189. This element is also found in revised substitute claim 26. *Kling* discloses this element as explained for substitute claim element [26b].

5. [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;”

190. This element is also found in revised substitute claim 26. *Kling* and *Lim* disclose this element as explained for revised substitute claim element [26c].

6. [41e] “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.”

191. This element is also found in revised substitute claim 26. *Kling* and *Lim* disclose this element as explained for revised substitute claim element [26d].

X. THE PETITION GROUNDS WITH *ZHA* AS PRIMARY REFERENCE

A. Obviousness under 35 U.S.C. § 103

192. In my declaration submitted in support of the Petition (Ex. 1002), I provided my opinion that claims 1-5, 9-10, 13-16, and 23-25 are unpatentable based on certain grounds (Grounds 1-6) in view of *Zha* (U.S. Patent No. 9,497,565 (Ex. 1004)) along with the POSITA’s knowledge and/or other prior art references (“*Zha* Grounds”). *See* Ex. 1002 ¶ 50.

193. It is my opinion that Patent Owner’s amendments to revised substitute claims 26-41 do not overcome the *Zha* Grounds and that these revised substitute claims remain obvious to a person of ordinary skill in the art.

1. Revised Substitute Claims 26 and 41

194. Revised substitute claims 26 and 41 are amended to add a new term “application specific authentication information that is not authentication information specific to a device” and to specify that “the application specific authentication information used on the first device is different from the application specific authentication information used on the second device” ([26c], [41d]).

195. Based on Patent Owner’s apparent understanding of the new limitations in revised substitute claims 26 and 41, it is my opinion that a POSITA would find these additional limitations obvious in view of *Zha* and their own general knowledge.

196. I evaluate the patentability of the revised substitute claims based on Patent Owner’s apparent reliance on the disclosure of using two different specific passwords to authenticate the first and second devices. In view of this assumption, it was well known by 2014 that password authentication could be used for logging into an application such as *Zha*’s microblog (e.g., Facebook login). In fact, a 2006 article co-authored by Patent Owner’s expert, Dr. Patrick Traynor, confirms that “[p]asswords are currently the dominant authentication mechanism in computing systems.” Ex. 1024 at 37 (PDF page 1). Accordingly, a person of ordinary skill in the art would know that passwords were the likely authentication mechanism for *Zha*’s disclosure that the “user may login to a microblog in the laptop computer, the

cellphone and the desktop computer with one microblog account” (Ex. 1004, 6:56-61). Thus, to the extent Patent Owner relies on password information as the “application specific authentication information that is not authentication information specific to a device,” using passwords with *Zha* would be obvious to a person of ordinary skill in the art. The passwords are not device specific because *Zha* does not disclose that the logins from the two terminals are specific to those two terminals.

197. In addition, a POSITA would understand that different authentication information (i.e., different passwords) could be used for the first and second devices. Evidence of this general knowledge is found in U.S. Patent No. 7,676,829 (“*Gui*”), which was filed in 2001 and issued in 2010, which teaches that different passwords could be used in systems providing access to different information having varying degrees of sensitivity (e.g., some less sensitive information and some more sensitive information). In particular, *Gui* discloses:

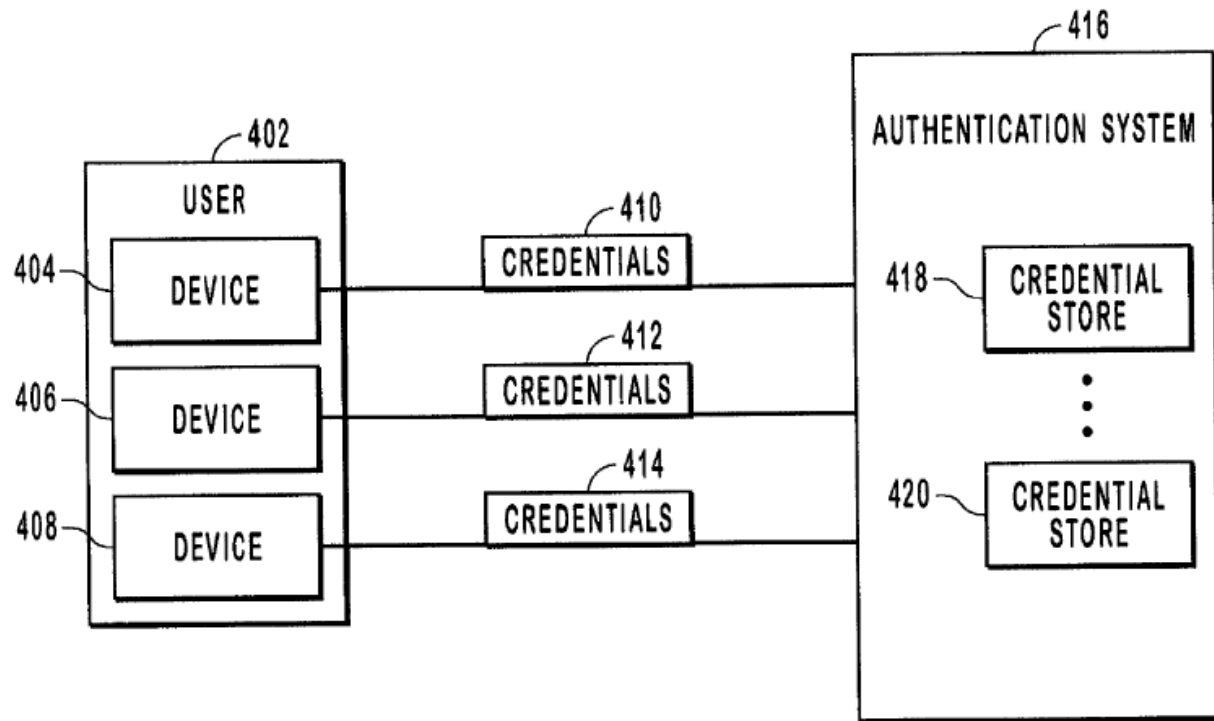


FIG. 4

FIG. 4 is a block diagram that illustrates how multiple credentials can be used in a distributed authentication system to authenticate a user to various services. FIG. 4 illustrates a user 402 that has one or more access devices that are represented by device 404, device 406, and device 408. The device 404 may be a desktop computer, while the device 406 is a PDA and the device 408 is a cellular telephone.

Ex. 1031, 9:11-17.

These and other problems are overcome by the present invention which provides systems and methods for the association of multiple sets of credentials to a single user account. An authentication system is provided that allows a user to be authenticated using different credentials. Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

Ex. 1031, 2:20-29.

One advantage of the present invention is the ability to associate multiple sets of credentials in a distributed authentication system such that a user can uniquely identify themselves to computer-based services using credentials that are most appropriate for a particular computer-based service and/or access device. Thus, a user can obtain access to a particular service when they use one credential from a device such as a cellular telephone and another credential from a different device such as a laptop computer.

Ex. 1031, 6:65-7:6.

Another advantage is the ability of the user to have credentials of varying security levels. Because high security credentials are often burdensome to users as well as on the authentication system, a user can associate credentials of varying security levels with a single user account. When a particular site is accessed, the site can specify the level of security that is required.

Ex. 1031, 2:55-61.

198. These disclosures in *Gui* confirm that a POSITA would understand to use different passwords where different devices have different keyboards or user interfaces to enter credentials and/or a website has varying security levels

199. Additionally, *Gui* addresses the same concern that allegedly motivated the '376 Patent, i.e., security. And like the '376 Patent, *Gui* further discusses “some credentials provide better security than other credentials. Numerical credentials, for instance, do not provide as much security as alphanumerical credentials or digital certificates/signatures. However, other security measures can be placed on these credentials.” Ex. 1031, 8:34-38. Thus, a POSITA’s general knowledge would include knowing that multiple passwords could be used to improve security in systems with sensitive information (e.g., *Zha*’s Microblog that includes private

messages). Thus, when faced with the alleged problem identified by Patent Owner (security), it would have been obvious to a POSITA to use a different password to access *Zha*'s more sensitive information (e.g., private messages).

200. U.S. Patent No. 7,865,950 ("*Lipetz*"), which was filed in 2007 and issued in 2001, is further evidence of a POSITA's general knowledge that different passwords could be used in systems providing access to different information having varying degrees of sensitivity (e.g., some less sensitive information and some more sensitive information). In particular, *Lipetz* discloses:

A data processing system includes a data storage unit for storing data sets accessible to a user upon receipt of permission. The data processing system restricts access to data sets by requiring a username and then requiring a password to obtain permission for access to a data set stored in a data storage unit. ***The system is adapted to support use of more than one said password associated with a username; and each of those passwords associated with that username permits a distinct level of access to a particular data set,*** whereas other passwords can provide different levels of access to any data set assigned thereto.

Ex. 1025, Abstract (emphasis added).

In accordance with this invention, a username is associated with multiple passwords; and the user has one username. Preferably, ***a single password allows access as normal with all privileges as normal; and also associated with the same username is another, auxiliary password which has fewer privileges.*** Further in accordance with this invention, the user is able to set up a plurality of passwords with different privileges granted to the user for different passwords depending upon the comfort level the user has with respect to the machine being used at the time; and the exact privileges can be determined by the user or the web site at the time of creation of the username.

Ex. 1025, 4:37-49 (emphasis added).

201. These disclosures in *Lipetz* confirm that a POSITA would understand to use different passwords where varying degrees of access to information is desired. Indeed, *Lipetz* provides the motivation to use this knowledge in other systems: “[t]his invention can be applied to any password based framework.” Ex. 1025, 6:47-48

202. Additionally, *Lipetz* addresses the same concern that allegedly motivated the ’376 Patent, i.e., malware. Ex. 1025, 1:63-66 (“A security problem exists because the user is usually unaware of what *malware*, spyware, key loggers, or any other security holes there may be in the system.” (emphasis added)). And like the ’376 Patent, *Lipetz* further discusses the malware problem in the context of a banking application. Ex. 1025, 2:3-16. Thus, a POSITA’s general knowledge would include knowing that multiple passwords could be used to defend against malware in systems with sensitive information (e.g., *Zha*’s Microblog that includes private messages). Thus, when faced with the alleged problem identified by Patent Owner (malware), it would have been obvious to a POSITA to use a different password to access *Zha*’s more sensitive information (e.g., private messages).

203. Evidence of this general knowledge is also found in *Kling*, which discloses an online banking system that allows a user to login with different devices such as a PC and a mobile device. Ex. 1023, [0013]-[0019]. *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. 1023, [0018]. *Kling*, a patent application filed in 2011 and published in 2012, confirms that logging into a multiple-device system containing sensitive information (e.g., bank account information) would “typically” and “ideally” use different authentication information (i.e., different passwords) on the two different devices. That *Kling* does not go into any further detail on the mechanics or functionality of using two different passwords in a multi-device system is further evidence that such details were well within the POSITA’s general knowledge in 2014.

204. Additionally, *Kling* addresses the same concern that allegedly motivated the ’376 Patent, i.e., malware. Ex. 1023, [0015]-[0016]. Thus, a POSITA’s general knowledge would include knowing that multiple passwords could be used to defend against malware in computer systems, including systems with multiple devices accessing the same application (e.g., *Zha*). Thus, when faced with the alleged problem identified by Patent Owner (malware), it would have been obvious to a POSITA to use a different password for each device in the system.

205. Counsel has informed me that any need or problem known in the field of endeavor at the time of the invention and addressed by the patent can provide a reason for combining the elements in the manner claimed. Counsel has also informed me that universal motivations to improve technology within a particular

field can provide a motivation to combine even absent any hint or suggestion in the references themselves.

206. Here, *Gui*, *Lipetz*, and *Kling* are prior art patents that relate to the field of computer security, and more particularly, to securing computer systems against malware. *See* Ex. 1031, 2:55-61 (“credentials of varying security levels”); Ex. 1025, 1:6-7 (“invention relates to provide software security”), 1:63-66 (“A security problem exists because the user is usually unaware of what malware, spyware, key loggers, or any other security holes there may be in the system.”); Ex. 1023, [0005] (“enhanced online transaction security”), [0015] (“the user’s local PC is compromised by Malware”). Thus, *Gui*, *Lipetz*, and *Kling* address the same concern the ’376 Patent purports to address. *See* Ex. 1001, 1:15-16 (“securing communications against malware”); Ex. 2004 ¶ 56 (Traynor declaration). Consequently, *Gui*, *Lipetz*, and *Kling* provide a motivation to combine a POSITA’s knowledge of using different passwords with *Zha*’s microblog application—i.e., to enhance security against malware in a computing system using multiple devices.

207. It is my opinion that adding different passwords to *Zha*’s microblog application would not be beyond the POSITA’s skill and that the POSITA would be motivated to modify *Zha* in this manner with a reasonable expectation of success. In fact, it is my opinion that *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 in an application was well within the POSITA’s knowledge before 2014.

208. For the above reasons, it is my opinion a POSITA would use the POSITA’s knowledge of multiple-password authentication schemes (as evidenced by *Gui*, *Lipetz*, and *Kling*) along with *Zha*’s microblog application, alone or as modified by prior art in the other *Zha* Grounds. In other words, a POSITA would be motivated to modify *Zha* to require at least two passwords, one for access to sensitive information on one device (e.g., private messages on the cellphone), and one for access to other information (e.g., homepage information on the laptop). This modification of *Zha* represents the simple substitution of one known element (single password associated with a single account) for another known element (multiple passwords associated with a single account) to obtain predictable results (enhanced security against malware). Put another way, use of the POSITA’s knowledge of multiple-password authentication schemes (as evidenced by *Gui*, *Lipetz*, and *Kling*) is the use of a known technique (multiple password authentication) to improve similar devices (computer systems) in the same way (protecting against malware by requiring multiple passwords).

209. Finally, *Gui* provides additional motivation to use multiple passwords in a system such as *Zha* that utilizes different hardware devices—human interface accessibility. Specifically, *Gui* explains:

One problem that often presents itself in these situations is related to the access devices that are used to access a computer based service. More specifically, the problem is related to the credentials that a user must supply in order to sign or log in to a computer based service. Credentials have to be entered into the access device when a user is signing in to a computer based service. Different devices have different form factors as well as different data input capabilities and while providing credentials on one device may be a relatively straightforward task, providing the same credentials on another device may prove to be a burdensome task.

For example, assume that a user has an email account and that the user is able to access the email account using the following credential:

Username: Joe@emailservice.com

Password: myPAssword.

When the user attempts to access their email account from a desktop computer, the credential can be quickly and easily entered using the keyboard because the user is able to quickly and easily select and enter upper/lower case letters as well as special characters. In contrast, when the user attempts to access their email account from their cellular phone, the task of logging in by entering this credential becomes significantly more difficult. The user is typically required to “triple-tap” on the numbers in order to select each letter in both the username and the password, navigate complex menu systems to select upper/lower case letters, and find symbols such as the “@” character. If the user desires to access their email account from their cellular phone, then the user is required to spend the time needed to enter the credential on the input restricted device because the email account can only be accessed with this credential.

Ex. 1031, 1:39-2:3.

210. As evidenced by *Gui*’s disclosure, a POSITA’s knowledge includes the understanding of the benefit of allowing multiple different passwords in a system

like *Zha* that provides for easy human interface access via desktop computer and mobile phone. Consequently, a POSITA would find it obvious based on this knowledge to allow the user to use different passwords on the different devices when logging into *Zha*'s microblog.

211. It is my opinion that a POSITA being motivated to modify *Zha* to include multiple different passwords for the same user account renders revised substitute claims 26 and 41 obvious for the same reasons discussed in my first declaration (Ex. 1002) for claims 1 and 25, respectively, for Grounds 1-2, and my second declaration (Ex. 1027) for substitute claims 26 and 41, respectively, for Grounds 1-6. It is my further opinion that using the POSITA's knowledge of multiple/different password authentication would not affect the combination of *Zha* with (1) other POSITA knowledge (Ground 1) or (2) *Tsushima* (Ground 2). A POSITA would have a reasonable expectation of success in implementing multiple passwords along with the other modifications to *Zha* and/or *Zha/Tsushima* because implementing the multiple password authentication would be trivial (e.g., requiring a minimal amount of additional information stored in an authentication database).

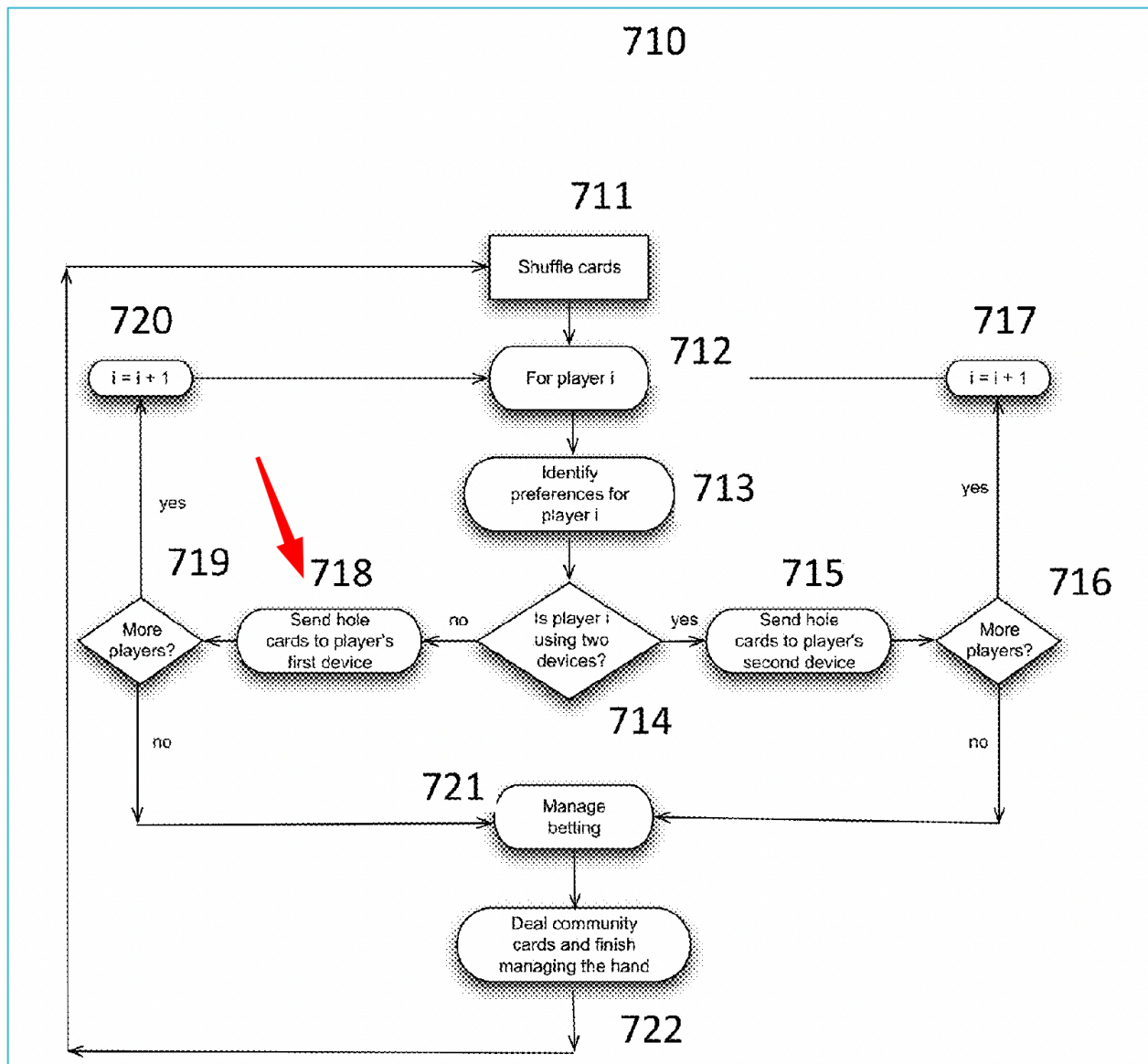
212. Patent Owner argues, "*Zha*'s microblog allows one password to access all the interfaces of the microblog on a single device. Ex. 2008, ¶¶99-100." RMTA at 13 (citing *Zha* at 14:6-12). I disagree. The cited passage reads as follows:

The terminals each send a login request to the server, the server returns contents in a main interface to each terminal after receiving the login

request, and the user performs a certain operation on the main interface to guide the terminal to each functional interface after the terminal displays the contents in the main interface.

213. *Zha* teaches each terminal has the option to select any functional interface. But *Zha* does not teach or suggest that the server actually assigns all functional interfaces to a single terminal.

214. Even if *Zha* teaches an embodiment where all information is transmitted to a single device, I understand that prior art references are to be considered for all they teach to a POSITA. A single-device embodiment would not detract from *Zha*'s disclosure of embodiments wherein sensitive and non-sensitive information is transmitted to different devices in a two-device embodiment. For example, the '376 Patent also teaches sending all information, including sensitive information, to one device. This is depicted, for example, at step 718 "Send hole cards to player's first device" in Figure 7 of the '376 Patent:



Ex. 1001, Figure 7 (red arrow added). A single-device embodiment where all information, including sensitive information, is transmitted to a single device would not somehow erase from the POSITA's understanding of *Zha* the disclosure of a two-device embodiment wherein sensitive information is transmitted to a first device, and non-sensitive information is transmitted to a second device.

2. Revised Substitute Claims 27-29, 31-34, and 36-40

215. I understand that revised substitute dependent claims 27-29, 31-34, and 36-40 are not modified from their corresponding original claims except that they ultimately depend from revised substitute independent claim 26. It is my opinion that these revised substitute claims would have been obvious to a POSITA based on the POSITA's knowledge of multiple/different password authentication schemes as evidenced by *Gui*, *Lipetz*, and *Kling* for the same reasons discussed in Section X.A (above).

3. Revised Substitute Claim 30

216. I understand Patent Owner's amendment to revised substitute claim 30 (original claim 5) includes depending from revised substitute claim 28 (original claim 3) instead of revised substitute claim 26 (original claim 1). It is my opinion that a POSITA would have found revised substitute claim 30 obvious based on the already-cited prior art and the POSITA's additional knowledge of multiple/different password authentication mechanisms as described by *Gui*, *Lipetz*, and *Kling*.

217. In particular, I previously explained why *Zha*, a POSITA's general knowledge, and *Gumbula* rendered original claim 5 obvious (Ground 3) and, alternatively, why *Zha*, a POSITA's general knowledge, *Tsushima*, and *Gumbula* rendered original claim 5 obvious (Ground 4). PO's amendment of this claim to depend from original claim 3 (reciting sensitive and non-sensitive information) does

not require additional argument, as *Zha* discloses the sensitive and non-sensitive information (see Petition Grounds 1-2). As discussed above, *Gui*, *Lipetz*, and *Kling* are evidence of the POSITA's further knowledge of using multiple/different passwords to improve security against malware when using different devices to access an online system. Section X.A (above). For the same reasons I discuss above, a POSITA would have a reasonable expectation of success in using this knowledge in combination with the other art I analyzed for Grounds 3 and 4.

218. Notably, neither Patent Owner nor its expert dispute that *Gumbula* is properly combined with the other prior art (e.g., *Zha*). As explained in my first declaration, *Gumbula* discloses “providing a notification on the second device that the connectivity has been disrupted” (Ex. 1002 ¶¶ 156-71, 176-77). It is my opinion that *Gumbula* similarly discloses Patent Owner's new amendment to this claim language. In particular, *Gumbula* discloses to provide a notification on the client/terminal indicating a disruption to connectivity. “If either client 12 or the server component 14 does not see a heartbeat message during the check interval then ***the client 12 displays the message ‘Lost connection to the server, retrying . . .’***” and the server component 14 sends a message to the agent 20 ‘Client has lost connection to the server, retrying . . .’. Ex. 1011, 4:44-49 (emphasis added). The *Gumbula* “lost connection” message provided by the client on the client device corresponds to “providing a notification on the second device that the connectivity

has been disrupted,” as claimed. *Gumbula* discloses the client may be a chat client running inside a web browser on the client device (e.g., Ex. 1011, Figure 1), and this chat client corresponds to “the application on the second device” that provides the notification in substitute/amended claim 30. Thus, the subject matter of substitute claim 30 is rendered obvious by *Zha*, a POSITA’s general knowledge, and *Gumbula* (Ground 3 with multiple/different passwords) or, alternatively, by *Zha*, a POSITA’s general knowledge, *Tsushima*, and *Gumbula* (Ground 4 with multiple/different passwords).

4. Revised Substitute Claim 35

219. I understand Patent Owner’s amendment to revised substitute claim 35 (original claim 14) includes (1) depending from substitute claim 30 (original claim 5) instead of substitute claim 26 (original claim 1); and (2) adding the limitation “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.” I discuss above my opinion as to why claim 28, from which claim 35 depends, lacks written description support. As a dependent claim, substitute claim 35 has the same defects. Regardless, it is my opinion that a POSITA would have found substitute claim 35 obvious based on the already-cited prior art and the POSITA’s additional knowledge of multiple/different

password authentication mechanisms as described by *Gui*, *Lipetz*, and *Kling*. Section X.A (above).

220. The limitation added to substitute claim 35 is identical to the limitation that was found in original claim 10. I previously explained why *Zha*, a POSITA's general knowledge, and *Stafford* render original claim 10 obvious (Ground 5 (Ex. 1002 ¶¶ 178-94)) and, alternatively, why *Zha*, a POSITA's general knowledge, *Tsushima*, and *Stafford* render original claim 10 obvious (Ground 6 (Ex. 1002 ¶¶ 195-196)).

221. Notably, neither Patent Owner nor its expert dispute that *Stafford* is properly combined with the other prior art (e.g., *Zha*). As explained in my first declaration, *Stafford* discloses “displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.” (Ex. 1002 ¶¶ 178-96). Patent Owner did not dispute this. Thus, *Stafford* discloses the same limitation found in amended/substitute claim 35 for the same, undisputed reasons.

222. For the foregoing reasons, it is my opinion that the subject matter of substitute claim 35 is rendered obvious by *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*). A POSITA would be motivated to combine *Gumbula* with *Zha*'s private messaging interface as explained for Petition Grounds 3-4, and would be motivated to combine *Stafford* with *Zha*'s game interface as explained for Petition Grounds 5-6. 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 have a reasonable expectation of success in making 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 disruption of connection in the messaging interface and providing a visual link between two devices in a game interface).

B. Response to Patent Owner's Arguments Related to *Zha* Grounds

1. "authentication information"

223. Patent Owner and its expert argue that "*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. Revised Motion to Amend ("RMTA") at 13; Ex. 2004 ¶ 52. I disagree. *Zha* discloses that the "user may login

to a microblog in the laptop computer, the cellphone, and the desktop computer with one microblog account.” Ex. 1004, 6:56-61. A POSITA would understand *Zha*’s disclosure of logging into a microblog application (e.g., Facebook or Twitter) could (and most likely would) be by means of entering a username and password. Indeed, even before 2014, the use of “[p]assword-based authentication mechanisms were the primary means by which users gain legitimate access to computing systems.” Ex. 1024 at 37 (PDF page 1). A POSITA would understand the password to be “authentication information” according to the revised amended claims. Patent Owner’s expert agrees with this conclusion. Ex. 1026, 71:9-17, 98:22-99:22. Further, *Gui*, *Lipetz*, and *Kling* are evidence of the POSITA’s further knowledge of using multiple/different passwords when logging into multiple devices to improve security against malware in an online system. The ongoing need to improve online security provides ample motivation for the POSITA to apply different login credentials to login to the *Zha* microblog via a laptop computer, a cellphone, and a desktop computer with one microblog account. *Gui* further motivates the POSITA to use different authentication information based on the accessibility of the different human interfaces of the *Zha* laptop computer, cellphone, and desktop computer. Thus, *Zha*’s disclosure of logging into the microblog, in view of the POSITA’s knowledge shown by *Gui*, *Lipetz*, and *Kling*, renders obvious using application

specific authentication information that is different for determining login to the application at the first and second devices.

224. In particular, *Gui* is evidence of a POSITA's general knowledge that different passwords are used in systems providing access to different information having varying degrees of sensitivity (e.g., some less sensitive information and some more sensitive information). *Gui* discloses:

These and other problems are overcome by the present invention which provides systems and methods for the association of multiple sets of credentials to a single user account. An authentication system is provided that allows a user to be authenticated using different credentials. Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

Ex. 1031, 2:20-29.

One advantage of the present invention is the ability to associate multiple sets of credentials in a distributed authentication system such that a user can uniquely identify themselves to computer-based services using credentials that are most appropriate for a particular computer-based service and/or access device. Thus, a user can obtain access to a particular service when they use one credential from a device such as a cellular telephone and another credential from a different device such as a laptop computer.

Ex. 1031, 6:65-7:6.

Another advantage is the ability of the user to have credentials of varying security levels. Because high security credentials are often burdensome to users as well as on the authentication system, a user can associate credentials of varying security levels with a single user account. When a particular site is accessed, the site can specify the level of security that is required.

Ex. 1031, 2:55-61.

225. These disclosures in *Gui* confirm that a POSITA would have understood to use different passwords where different devices have different keyboards or user interfaces to enter credentials and/or a website has varying security levels.

226. Additionally, *Gui* addresses the same concern that allegedly motivated the '376 Patent, i.e., security. And like the '376 Patent, *Gui* further discusses “some credentials provide better security than other credentials. Numerical credentials, for instance, do not provide as much security as alphanumerical credentials or digital certificates/signatures. However, other security measures can be placed on these credentials.” Ex. 1031, 8:34-38. Thus, a POSITA’s general knowledge would have included knowing that multiple passwords could be used to improve security in systems with sensitive information (e.g., *Zha*’s Microblog that includes private messages). Thus, when faced with the alleged problem identified by Patent Owner (security), it would have been obvious to a POSITA to use a different password to access *Zha*’s more sensitive information (e.g., private messages).

227. *Lipetz* is further evidence of a POSITA’s general knowledge that different passwords were used in systems providing access to different information having varying degrees of sensitivity (e.g., some less sensitive information and some more sensitive information). In particular, *Lipetz* discloses:

A data processing system includes a data storage unit for storing data sets accessible to a user upon receipt of permission. The data processing system restricts access to data sets by requiring a username and then requiring a password to obtain permission for access to a data set stored in a data storage unit. ***The system is adapted to support use of more than one said password associated with a username; and each of those passwords associated with that username permits a distinct level of access to a particular data set,*** whereas other passwords can provide different levels of access to any data set assigned thereto.

Ex. 1025, Abstract (emphasis added).

In accordance with this invention, a username is associated with multiple passwords; and the user has one username. Preferably, ***a single password allows access as normal with all privileges as normal; and also associated with the same username is another, auxiliary password which has fewer privileges.*** Further in accordance with this invention, the user is able to set up a plurality of passwords with different privileges granted to the user for different passwords depending upon the comfort level the user has with respect to the machine being used at the time; and the exact privileges can be determined by the user or the web site at the time of creation of the username.

Ex. 1025, 4:37-49 (emphasis added). These disclosures in *Lipetz* confirm that a POSITA would have understood to use different passwords where varying degrees of access to information is desired. Indeed, *Lipetz* motivates to use this knowledge in other systems: “[t]his invention can be applied to any password based framework.” Ex. 1025, 6:47-48.

228. Additionally, *Lipetz* addresses the same concern that allegedly motivated the ’376 Patent, i.e., malware. Ex. 1025, 1:63-66 (“A security problem exists because the user is usually unaware of what ***malware***, spyware, key loggers,

or any other security holes there may be in the system.” (emphasis added)). And like the ’376 Patent, *Lipetz* further discusses the malware problem in the context of a banking application. Ex. 1025, 2:3-16. Thus, a POSITA’s general knowledge would include knowing that multiple passwords could be used to defend against malware in systems with sensitive information (e.g., *Zha*’s microblog application that includes sensitive, user-specific information (private message interface)). Thus, when faced with the alleged problem identified by Patent Owner (malware), it would have been obvious to a POSITA to use a different password to access *Zha*’s more sensitive information (e.g., private message interface).

229. Similarly, *Kling* teaches different login credentials on different devices. On a PC, “the user would open a Web site 202, in this example of a bank, [and be] prompted for a login and password 203, 204.” Ex. 1023, Figure 2, [0014]; Fig. 4, [0017] (“Steps 402-407 proceed just like the flow shown in FIG. 2.”); Figure 5, [0019] (“The initial login process 502-507 remains the same as previously described.”). Also, to the mobile device, “the bank server generates a secondary confirmation request 513, 514” (Ex. 1023, [0019]) comprising “display secondary login message 513” for the user to “enter login and password 514.” Ex. 1023, Figure 5. “Typically the user would be prompted to log into the mobile device, ideally using a different password than on the PC.” Ex. 1023, [0018]. For the user’s PC 400, *Kling* expressly shows the bank server 401 “authenticates user” on the PC 400 at step 405

after the user has “enter[ed] login and password” via the PC 400 at step 407. For the user’s secondary mobile phone 412, *Kling* does not expressly show an authentication step by the server, but a POSITA would understand the server similarly “authenticates user” on the secondary mobile phone 412 after the user has “enter[ed] login and password” via the secondary mobile phone 412 at step 414.

230. Thus, *Zha*’s disclosure of logging into the microblog, in view of the POSITA’s knowledge shown by *Gui*, *Lipetz*, and *Kling*, renders obvious using application specific authentication information that is different for determining login to the application at the first and second devices.

2. Preamble and “thereby” limitation [d]

231. Patent Owner and its expert argue *Zha* does not meet the revised amended preamble and “thereby” limitation [d] that allegedly require enhanced data protection. RMTA at 16; Ex. 2008, ¶¶106-107. In particular, it is argued “*Zha* does not disclose protecting information at all.” *Id.* I disagree. First, PO’s revised claims 26 and 41 to recite, “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.” However, this “thereby” clause merely states the result of the limitations in claims 26 and 41 and does not further limit claims 26 and 41, as discussed above. Regardless, a POSITA would understand *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 to the user's phone, that information will be protected from malware on the user's desktop computer while that setting remains. .

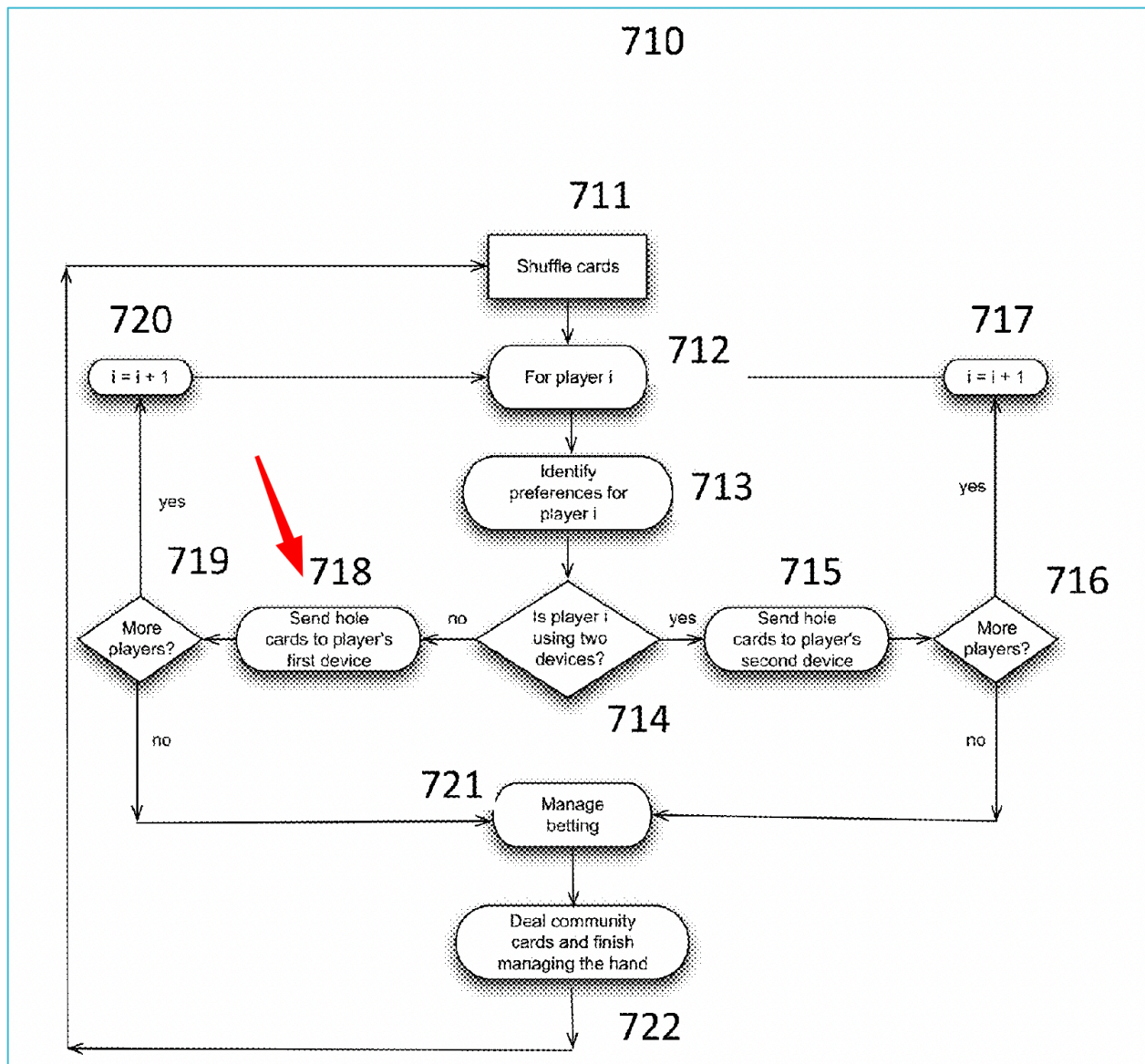
3. “sensitive information is only shared with the second device”

232. Patent Owner and its expert argue that *Zha* does not disclose “sensitive information is only shared with the second device,” as claimed in revised amended substitute claim 28. RMTA at 17; Ex. 2008 ¶¶ 109-13. In particular, it is argued (1) the *Zha* private messages are by definition shared beyond the second device (i.e., “messages between individuals [require] sharing the sensitive information beyond the second device” (Ex. 2008, ¶ 112)), and (2) the private chat app is accessible on the first device. *Id.* I disagree with these arguments.

233. The first argument contradicts every embodiment disclosed in the '376 Patent and thus makes little sense in the context of the claims. Thus, a POSITA certainly would not understand this new amendment to mean what PO argues it means. In particular, 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. In addition, all of this information originates at the server, so it is also shared with the server. The '376 Patent discloses each of these examples (hole cards, banking information, health

information) as sensitive information. As such, a POSITA would view this new amended limitation, “only shared with the second device,” in the context of the claim and specification to mean to the exclusion of the first device (i.e., not shared with the first device)—not “not ever shared with any other device other than the second device.” With this understanding, *Zha*’s private messages, in the embodiment where *Zha* is configured to send private messages to the user’s cell phone, renders this claim obvious.

234. As to the second argument, even if *Zha* teaches one embodiment where all information, including sensitive information, is shared with a single device, that does not preclude *Zha*’s teaching of other embodiments that only share sensitive information with a second device. *Zha* teaches one-device and two-device embodiments similarly to how the ’376 Patent teaches one-device and two-device embodiments. A POSITA understands that if a user of *Zha*’s microblog has only one device (e.g., a laptop computer), private messages will be sent to that device. Likewise, the ’376 Patent discloses that if there is only one device (i.e., the first device), the sensitive information is sent to the first device. This is depicted, for example, at step 718 “Send hole cards to player’s first device” in Figure 7 of the ’376 Patent:



Ex. 1001, Figure 7 (red arrow added).

235. Similarly, a POSITA understands that a user can use a second device (e.g., a cellphone) with *Zha*'s microblog application and configure the application to send the private messages to the cellphone. Ex. 1004, 18:66-19:13. In this scenario, a POSITA understands that *Zha* will not send private messages to the laptop until the user specifically allows that to happen by re-configuring the access permissions (i.e., giving the application permission to send the private messages to the laptop).

Id. A POSITA understands that the '376 Patent discloses the same type of arrangement where “the user can elect to switch to not using two devices, if the user is willing to assume the risk and wants to continue play” when a connection to the second device is unavailable.

[34] If the game server remains unable to communicate with the second device, the game server can indicate to the first device that the second device is unavailable, and the first device can display a warning to the user that the second device is not reachable. In this event, the poker game can proceed. For example, if the second device is not reachable from the game server, the user can be forced to sit out until such time as the user's two devices are reachable. At any point, the user can elect to switch to not using two devices, if the user is willing to assume the risk and wants to continue to play.

Ex. 2005-008 -009.

236. Because *Zha* works in substantially the same way as the '376 Patent (both one-device and two-device embodiments are disclosed), it is my opinion that *Zha*'s two-device embodiment satisfies “sensitive information is only shared with the second device.”

XI. ADDITIONAL GROUNDS: *ZHA* GROUNDS COMBINED WITH *GUI*

237. In my declaration submitted in support of the Petition (Ex. 1002), I provided my opinion that claims 1-5, 9-10, 13-16, and 23-25 are unpatentable based on the *Zha* Grounds. *See* Ex. 1002 ¶ 50 (Grounds 1-6).

238. It is my opinion a POSITA would be motivated to combine *Gui* with the other prior art (Grounds 1-6) for the same reasons I provide above in Section

X.A, which I incorporate herein by reference. Consequently, it is my opinion that substitute claims 26-41 are unpatentable based on the *Zha* Grounds as modified by *Gui*'s disclosure of using multiple/different passwords with different devices. This combination uses *Gui*'s teaching of why an application might use different passwords for different devices to render the revised substitute claims obvious in view of *Zha* and *Gui*. This combination does not require the full implementation of *Gui*'s distributed credential system (e.g., *Gui* Figure 3) in combination with *Zha*. In other words, a POSITA would simply modify *Zha* so that the microblog application allows different passwords to access the same user account, for the reasons taught by *Gui*. *Zha*'s microblog application would handle the device authentication just as *Gui* Figure 2 shows the service (i.e., the application) handling the device authentication:

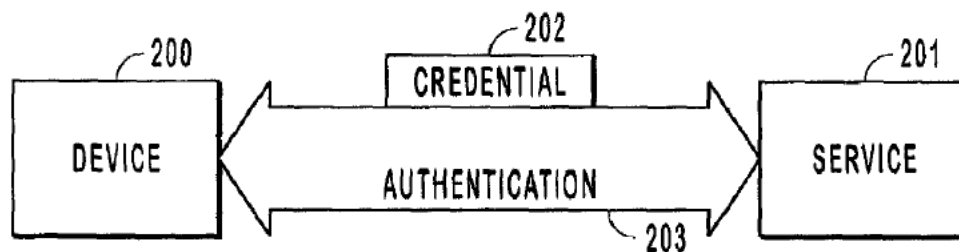


FIG. 2

Ex. 1031, Fig. 2.

239. Specifically, *Gui* provides express motivation to use different passwords for the different devices in a system such as *Zha*:

Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

Ex. 1031, 2:24-29.

240. *Gui* provides a detailed explanation as to why a POSITA would be motivated to use the different passwords:

One problem that often presents itself in these situations is related to the access devices that are used to access a computer based service. More specifically, the problem is related to the credentials that a user must supply in order to sign or log in to a computer based service. Credentials have to be entered into the access device when a user is signing in to a computer based service. Different devices have different form factors as well as different data input capabilities and while providing credentials on one device may be a relatively straightforward task, providing the same credentials on another device may prove to be a burdensome task.

For example, assume that a user has an email account and that the user is able to access the email account using the following credential:

Username: Joe@emailservice.com

Password: myPAssword.

When the user attempts to access their email account from a desktop computer, the credential can be quickly and easily entered using the keyboard because the user is able to quickly and easily select and enter upper/lower case letters as well as special characters. In contrast, when the user attempts to access their email account from their cellular phone, the task of logging in by entering this credential becomes significantly more difficult. The user is typically required to “triple-tap” on the numbers in order to select each letter in both the username and the password, navigate complex menu systems to select upper/lower case letters, and find symbols such as the “@” character. If the user

desires to access their email account from their cellular phone, then the user is required to spend the time needed to enter the credential on the input restricted device because the email account can only be accessed with this credential.

Ex. 1031, 1:39-2:3; *see also* Ex. 1031, 6:65-7:6.

241. In other words, at the time of the '376 Patent (in fact, earlier), *Gui* teaches that some passwords are more difficult to enter on a mobile phone compared to entering the same password on a computer that has a full keyboard. *Gui* suggests an easy solution to this problem for any service that allows login to the same account by both mobile phones and desktop/laptop computers. *Gui*'s solution is to allow the user to have multiple passwords for logging into the same account/service. I note that a POSITA would understand *Gui*'s use of the word "service" to be synonymous with the '376 Patent's use of the word "application" as *Gui* explains: "The explosive growth of the Internet and related technologies has resulted in a great number of computer based services that are available to consumers. Web portals, instant messaging, and email are examples of those services." Ex. 1031, 1:16-19.

242. If PO argues 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 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 "any device." *Id.*, 10:21-33.

243. 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 ¶¶212–218. 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 ¶¶213-16.

244. 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).

245. It is my opinion that 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*. In fact, it is my opinion that *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.

XII. THE PETITION GROUNDS WITH *TAKAHASHI* AS PRIMARY REFERENCE

A. Obviousness under 35 U.S.C. § 103

246. In my declaration submitted in support of the Petition (Ex. 1002), I provided my opinion that claims 1-5, 9-10, 12-14, 16-17, and 23-25 are unpatentable based on certain grounds (Grounds 7-8) in view of *Takahashi* (U.S. Patent Pub. No. 2015/0011318 (Ex. 1007)) along with the POSITA's knowledge and/or other prior art references ("*Takahashi* Grounds"). *See* Ex. 1002 ¶ 50. In my second declaration (Ex. 1027), I provided my opinion that the amended claims are unpatentable in view of the *Takahashi* Grounds, in support of Petitioner's Opposition to Patent Owner's Motion to amend.

247. It is my opinion that Patent Owner's revised amendments to substitute claims 26-35, 37-41 do not overcome the *Takahashi* Grounds and that these revised substitute claims remain obvious to a person of ordinary skill in the art.

1. Revised Substitute Claims 26 and 41

248. Revised substitute claims 26 and 41 are amended to add a new term "application specific authentication information that is not authentication information specific to a device" and to specify that "the application specific authentication information used on the first device is different from the application specific authentication information used on the second device" ([26c], [41d]).

249. Revised amended claim 26 requires that the user uses application specific authentication information that is not specific to a device. *Takahashi* teaches its system may be accessed with (1) a user ID and password OR (2) identification information (that is unique to each mobile terminal):

After receiving a HTTP request as access request from the mobile terminal 10 or the PC 12 of the user, the CPU 21 of the game server 20 identifies identification information, or user ID and a password, based on user agent character strings included in the HTTP request. The CPU 21 collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is one from any of the registered users, the CPU 21 accepts the access request.

Ex. 1007, ¶ [0095] (emphasis added). A POSITA reading this passage understands that *Takahashi*'s use of the word "or" means the user may login with (1) user ID and password or (2) identification information. A POSITA also understands that the user ID and password is not specific to a device, which corresponds to revised amended claim 26[c]. For this reason, it is my opinion that *Takahashi* expressly discloses the new limitations of revised substitute claims 26 and 41.

250. Alternatively, based on Patent Owner's apparent understanding of the new limitations in revised substitute claims 26 and 41, it is my opinion that a person of ordinary skill in the art would find these additional limitations obvious in view of *Takahashi* and their own general knowledge.

251. I evaluate the patentability of the revised substitute claims based on Patent Owner's apparent reliance on the disclosure of using two different passwords to authenticate the first and second devices. I note that *Takahashi* discloses the use of passwords as part of its authentication process:

In the authentication processing, the identification information, or the userID and the password, which are included in the HTTP request, are identified first. The game server 20 then collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is a request from any of the registered users, the game server 20 accepts the access request.

Ex. 1007, [0110].

User ID	Password	Identification Information	Terminal information of main-terminal	Terminal information of sub-terminal
012345	knm001	xxxxxxxxxx		

Ex. 1007, Figure 6 (red arrow added).

252. Thus, to the extent Patent Owner relies on password information as the “application specific authentication information,” using passwords with *Takahashi* is expressly disclosed.

253. In addition, a POSITA would understand that different authentication information (i.e., different passwords) could be used for *Takahashi*’s first and second devices. Evidence of this general knowledge is found in *Gui*, which discloses that different passwords could be used in systems providing access to different information having varying degrees of sensitivity (e.g., some less sensitive information and some more sensitive information) by multiple devices with different human interfaces exist. In particular, *Gui* discloses:

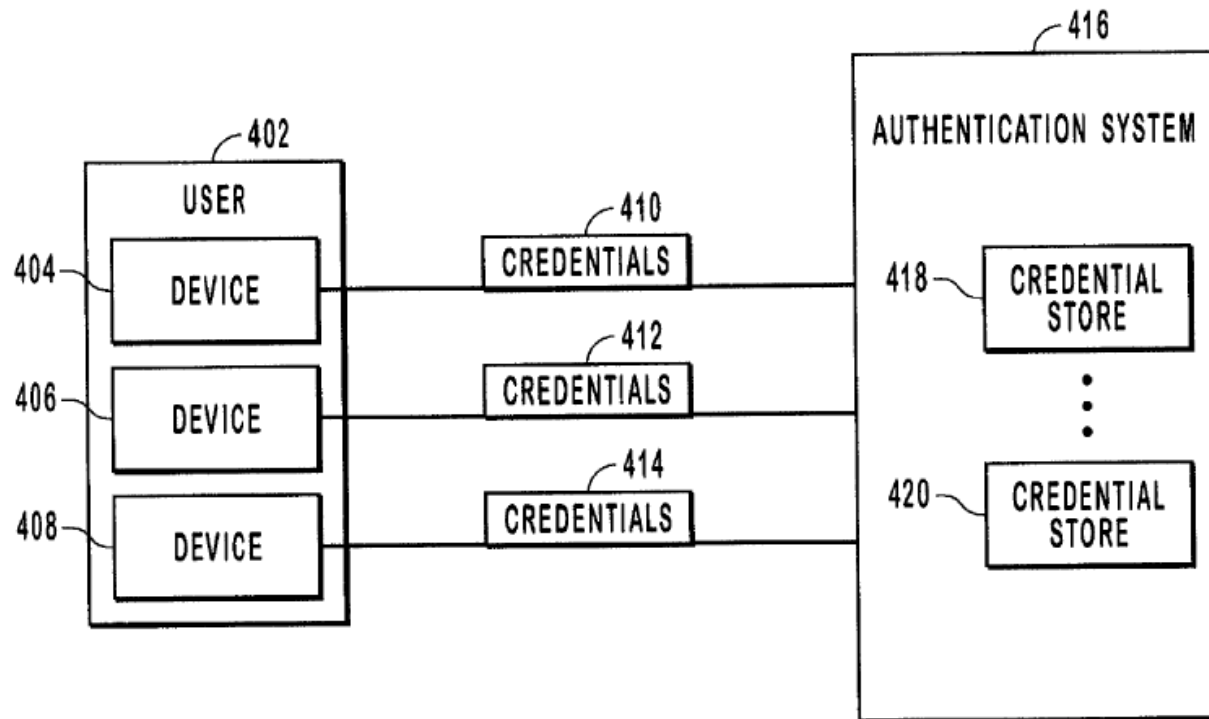


FIG. 4

FIG. 4 is a block diagram that illustrates how multiple credentials can be used in a distributed authentication system to authenticate a user to various services. FIG. 4 illustrates a user 402 that has one or more access devices that are represented by device 404, device 406, and device 408. The device 404 may be a desktop computer, while the device 406 is a PDA and the device 408 is a cellular telephone.

Ex. 1031, 9:11-17.

These and other problems are overcome by the present invention which provides systems and methods for the association of multiple sets of credentials to a single user account. An authentication system is provided that allows a user to be authenticated using different credentials. Thus, a user is able to be authenticated by the authentication system using the credential that is most appropriate for their access device. This enables the user to easily access computer based services using devices that have different form factors, data input techniques, and security capabilities.

Ex. 1031, 2:20-29.

One advantage of the present invention is the ability to associate multiple sets of credentials in a distributed authentication system such that a user can uniquely identify themselves to computer-based services using credentials that are most appropriate for a particular computer-based service and/or access device. Thus, a user can obtain access to a particular service when they use one credential from a device such as a cellular telephone and another credential from a different device such as a laptop computer.

Ex. 1031, 6:65-7:6.

Another advantage is the ability of the user to have credentials of varying security levels. Because high security credentials are often burdensome to users as well as on the authentication system, a user can associate credentials of varying security levels with a single user account. When a particular site is accessed, the site can specify the level of security that is required.

Ex. 1031, 2:55-61.

254. These disclosures in *Gui* confirm that a POSITA would understand to use different passwords where different devices have different keyboards or user interfaces to enter credentials and/or a website has varying security levels.

255. In addition, a POSITA would understand that different authentication information (i.e., different passwords) could be used for *Takahashi*'s first and second devices. Evidence of this general knowledge is found in *Kling*, which discloses an online banking system that allows a user to login with different devices such as a PC and a mobile device. Ex. 1023, [0013]-[0019]. *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. 1023, [0018]. *Kling*, a patent application filed in 2011 and published in 2012, confirms that logging into a multiple-device system would

“typically” and “ideally” use different authentication information (i.e., different passwords) on the two different devices. That *Kling* does not go into any further detail on the mechanics or functionality of using two different passwords in a multi-device system is further evidence that such details were well within the POSITA’s general knowledge in 2014.

256. Additionally, *Kling* addresses the same concern that allegedly motivated the ’376 Patent, i.e., malware. Ex. 1023, [0015]-[0016]. Thus, a POSITA’s general knowledge would include knowing that multiple passwords could be used to defend against malware in computer systems, including systems with multiple devices accessing the same application (e.g., *Takahashi*). Thus, when faced with the alleged problem identified by Patent Owner (malware), it would have been obvious to a POSITA to use a different password for each device in the system.

257. It is my opinion that adding different passwords to *Takahashi*’s game application would not be beyond the POSITA’s skill and that the POSITA would be motivated to modify *Takahashi* in this manner with a reasonable expectation of success. Indeed, *Gui*’s and *Kling*’s disclosure of different passwords in an application is high-level (and without much detail)—evidence that implementing a password authentication mechanism in an application was well within the POSITA’s knowledge before 2014.

258. For the above reasons, it is my opinion a POSITA would use the POSITA's knowledge of multiple-password authentication schemes (as evidenced by *Gui*) along with *Takahashi*'s game application, alone or as modified by prior art in the other *Takahashi* Grounds. In other words, a POSITA would be motivated to modify *Takahashi* to require at least two passwords, one for access to sensitive information on one device (e.g., user-specific information on the mobile terminal), and one for access to other information (e.g., non-user-specific information on the main terminal). This modification of *Takahashi* represents the simple substitution of one known element (single password associated with a single account) for another known element (multiple passwords associated with a single account) to obtain predictable results (enhanced security against malware). Put another way, use of the POSITA's knowledge of multiple-password authentication schemes (as evidenced by *Gui* and *Kling*) is the use of a known technique (multiple password authentication) to improve similar devices (computer systems) in the same way (protecting against malware by requiring multiple passwords and providing for easier password entry on mobile phone devices that have more limited input interfaces).

259. It is my opinion that this motivation to modify *Takahashi* to include multiple different passwords for the same user account renders revised substitute claims 26 and 41 obvious for the same reasons discussed in my first declaration (Ex.

1002) for claims 1 and 25, respectively, for Grounds 7-8. It is my further opinion that using the POSITA's knowledge of multiple/different password authentication would not affect the combination of *Takahashi* with (1) other POSITA knowledge (Ground 7) or (2) *Tsushima* (Ground 8). A POSITA would have a reasonable expectation of success in implementing multiple passwords along with the other modifications to *Takahashi* and/or *Takahashi/Tsushima* because implementing the multiple password authentication would be trivial (e.g., requiring a minimal amount of additional information stored in an authentication database). For example, a POSITA would know to modify Figure 6 of *Takahashi* to include a second password field for each user, to enforce a password policy that requires different passwords, and to check both password fields during the authentication process.

2. Revised Substitute Claims 27-29, 31-34, and 37-41

260. I understand that substitute dependent claims 27-29, 31-34, and 37-40 are not modified from their corresponding original claims except that they ultimately depend from substitute independent claim 26. It is my opinion that these substitute claims would have been obvious to a POSITA based on the POSITA's knowledge of multiple/different password authentication schemes as evidenced by *Gui* and *Kling* for the same reasons discussed in Section X.A (above).

3. Revised Substitute Claim 30

261. I understand Patent Owner's revised amendment to substitute claim 30 (original claim 5) is to depend from substitute claim 28 (original claim 3) instead of substitute claim 26 (original claim 1). I discuss above my opinion as to why claim 28, from which claim 30 depends, lacks written description support. As a dependent claim, substitute claim 35 has the same defects. Regardless, it is also my opinion that a POSITA would have found revised substitute claim 30 obvious based on the already-cited prior art (for original claim 5) and the POSITA's additional knowledge of multiple/different password authentication mechanisms as described by *Gui* and *Kling*.

262. In particular, I previously explained why *Takahashi* and a POSITA's general knowledge rendered original claim 5 obvious (Ground 7) and, alternatively, why *Takahashi*, a POSITA's general knowledge, and *Tsushima* rendered original claim 5 obvious (Ground 8). As discussed above, *Gui* and *Kling* are evidence of the POSITA's further knowledge of using multiple/different passwords (1) to make password entry easier on devices with constrained input interfaces, and (2) to improve security against malware when using different devices to access an online system. For the same reasons I discuss above, a POSITA would have a reasonable expectation of success in using this knowledge in combination with the other art I analyzed for Grounds 7 and 8.

263. It is my opinion that *Takahashi* similarly discloses Patent Owner's new revised amendment to this claim language, as best understood. In particular, *Takahashi* discloses a web-based fishing game that is executed in a web browser executing on a mobile terminal. Ex. 1007, [0046]. A web browser is an application on the mobile terminal device, and as I previously explained, the web browser will provide a notification to the mobile terminal (e.g., an HTTP status code) when the connection to the game server is disrupted. Ex. 1002 ¶¶ 265-66. Thus, the subject matter of substitute claim 30, "providing a notification by the application on the second device," is rendered obvious by *Takahashi* and a POSITA's general knowledge, and (Ground 7 with multiple/different passwords) or, alternatively, by *Takahashi*, a POSITA's general knowledge, and *Tsushima* (Ground 8 with multiple/different passwords).

4. Revised Substitute Claim 35

264. I understand Patent Owner's amendment to substitute claim 35 (original claim 14) includes (1) depending from substitute claim 30 (original claim 5) instead of substitute claim 26 (original claim 1); and (2) adding the limitation "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." I discuss above my opinion as to why claim 28, from which claim 35 depends, lacks written description support. As

a dependent claim, substitute claim 35 has the same defects. Regardless, it is also my opinion that a POSITA would have found substitute claim 35 obvious based on the already-cited prior art and the POSITA's additional knowledge of multiple/different password authentication mechanisms as described by *Gui* and *Kling*.

265. The limitation added to substitute claim 35 is identical to the limitation that was found in original claim 10. I previously explained why *Takahashi* and a POSITA's general knowledge render original claim 10 obvious (Ground 7 (Ex. 1002 ¶¶ 269-76)) and, alternatively, why *Takahashi*, a POSITA's general knowledge, and *Tsushima* render original claim 10 obvious (Ground 8 (Ex. 1002 ¶¶ 339-46)).

266. Notably, neither Patent Owner nor its expert dispute that *Takahashi* discloses “displaying a graphical identifier on the first device and a corresponding graphical indicator on the second device indicating a link between the information displayed on the respective devices.” (Ex. 1002 ¶¶ 269-76). Patent Owner did not dispute this. Thus, *Takahashi* discloses the same limitation found in amended/substitute claim 35 for the same, undisputed reasons.

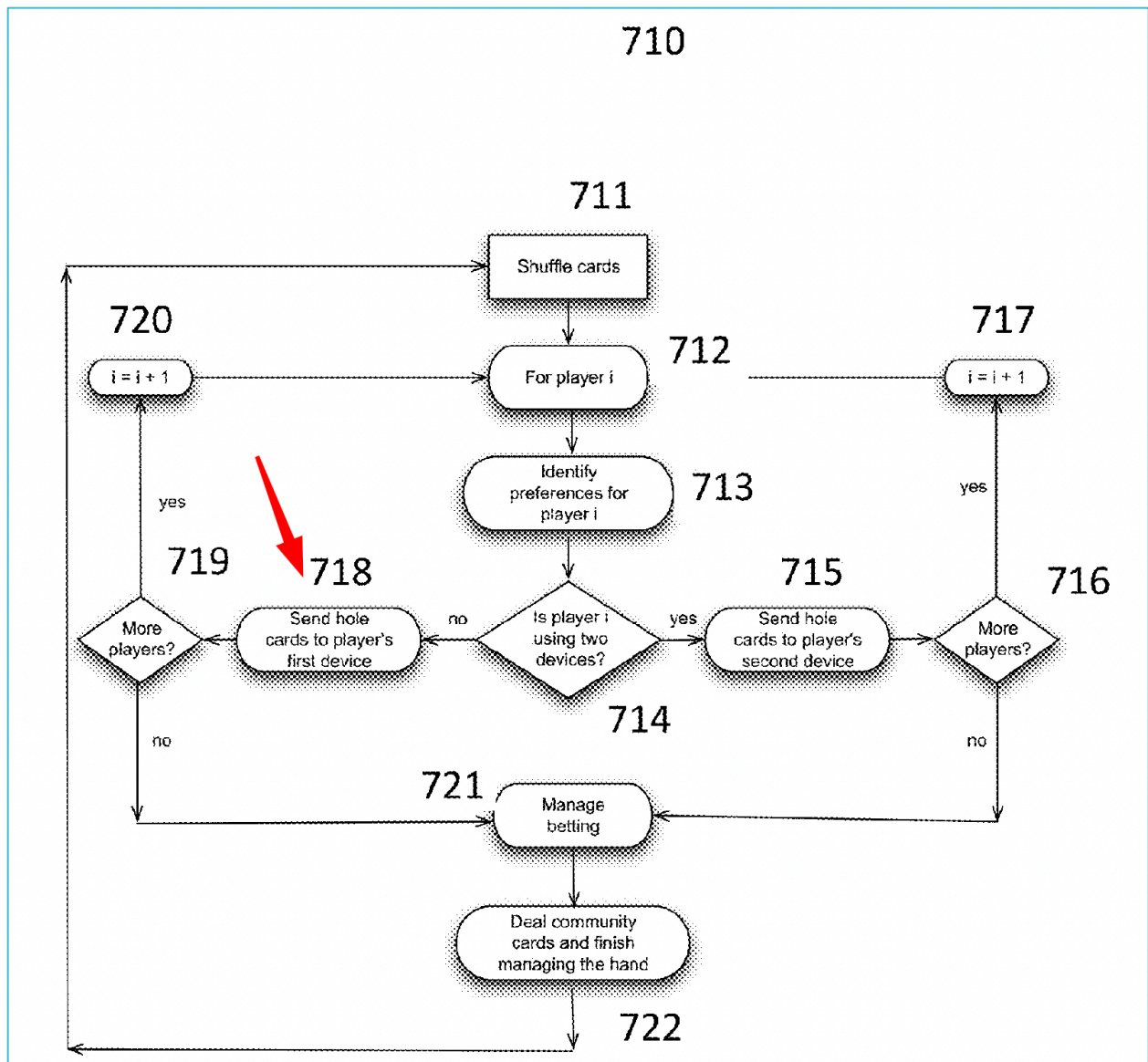
267. For the foregoing reasons, it is my opinion that the subject matter of substitute claim 35 is rendered obvious by *Takahashi* and a POSITA's general knowledge (Ground 7 and the POSITA's general knowledge of multiple/different passwords as disclosed in *Gui* and *Kling*) or, alternatively, by *Takahashi*, a

POSITA's general knowledge, and *Tsushima* (Ground 8 and the POSITA's general knowledge of multiple/different passwords as disclosed in *Gui* and *Kling*).

B. Response to Patent Owner's Arguments Related to *Takahashi* Grounds

1. Takahashi discloses revised substitute claims 26-35 and 37-41

268. In view of the revised substitute claims 26-35 and 37-41, 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. I disagree that *Takahashi's* disclosure of multiple embodiments somehow renders the teaching of the two-device embodiment a nullity, as Patent Owner appears to suggest. Even if *Takahashi* teaches a single-device embodiment where all information is transmitted to a single device, I understand that prior art references are to be considered for all they teach to a person of skill in the art. A single-device embodiment would not detract from *Takahashi's* disclosure of a two-device embodiment wherein sensitive and non-sensitive information is transmitted to different devices. Further, the '376 Patent also teaches sending all information, including sensitive information, to one device. This is depicted, for example, at step 718 "Send hole cards to player's first device" in Figure 7 of the '376 Patent:



269. Ex. 1001, Figure 7 (red arrow added). Like the '376 Patent, *Takahashi's* teaching of a single-device embodiment where all information, including sensitive information, is transmitted to a single device does not detract from its teaching of a two-device embodiment wherein sensitive information is transmitted to a first device, and non-sensitive information is transmitted to a second device.

**2. Login process followed by an authentication process
(revised substitute claim 26, limitation [c])**

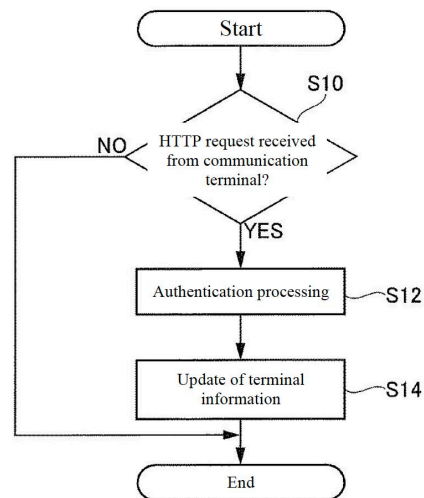
270. Patent Owner and its expert make an argument that *Takahashi*'s authentication processing is not part of the login process and that, for some unexplained reason, this results in *Takahashi* not disclosing the features of the substitute claims. RMTA at 19-20; Ex. 2008 ¶¶ 134-36. I disagree.

271. Patent Owner suggests that “*Takahashi* fails to disclose Substitute Claim limitation 26[c] because *Takahashi* discloses authenticating the user after the user has logged in.” RMTA at 20. Factually, I disagree with Patent Owner's understanding of *Takahashi*. Moreover, it is unclear what claim language Patent Owner is referring to or why Patent Owner believes a certain order is required. Nevertheless, it is my opinion that a POSITA would not understand *Takahashi* to perform authentication after the user has logged in. This would be non-sensical and is contrary to the POSITA's understanding of how login and authentication work.

272. Patent Owner and Dr. Traynor take an overly narrow view of *Takahashi*'s disclosure. A POSITA would understand that the entire process described in *Takahashi*, including the login and authentication processing, would have been part of a normal, well-known password login/authentication scheme at the time *Takahashi* was filed in 2012. A POSITA understands that the “login” of *Takahashi* represents the **input and transmission** of login credentials, i.e., the transmission of username and password. When referring to login authentication, the

first step would not be understood to complete the (or any) authentication—entering credentials is only a beginning of the process. Paragraph [0110] is very clear on this point: “After **receiving** the HTTP request (Step S10: YES), the game server 20 performs authentication processing (Step S12).” While the wording (which was originally in Japanese) may suggest two separate processes, a POSITA would understand the overall description of the process of Figure 11 to be normal password authentication where a username and password (and other “identification information”) are provided as part of the HTTP request in step S10 in Figure 11. Ex. 1007, [0110], Figure 11). The server then checks that information against the user data in the user database and grants access if there is a match. Ex. 1007, [0110]. There is nothing special about this description, which describes normal password authentication when a user logs into a system. I further note that in the certified English translation of *Takahashi*, Figure 11 is labeled “Processing at the time of login,” which further confirms that Figure 11 merely depicts a normal login process.

[Fig. 11]



 Processing at the time of login

Ex. 1009-57 (red arrow added).

273. Patent Owner and its expert make an argument that *Takahashi* specifically relies on device specific authentication information. RMTA at 20; Ex. 2008 ¶ 137. In particular, Patent Owner argues, “Dr. Rubin has further narrowed Substitute Claim limitation 26[c] to specifically exclude use of device specific authentication information.” *Id.* I disagree that *Takahashi* does not render the revised claim obvious.

274. Revised amended claim 26 recites, “determining . . . based on the first user being logged into the application using application specific authentication

information that is not authentication information specific to a device.” Revised amended claim 26 does not preclude use of device specific information. Rather, revised amended claim 26 merely requires that the user uses application specific authentication information that is not specific to a device. *Takahashi* teaches its system may be accessed with (1) a user ID and password OR (2) identification information (that is unique to each mobile terminal):

After receiving a HTTP request as access request from the mobile terminal 10 or the PC 12 of the user, the CPU 21 of the game server 20 identifies identification information, or user ID and a password, based on user agent character strings included in the HTTP request. The CPU 21 collates the identified identification information, or the identified user ID and the identified password, with the identification information, or the user ID and the password recorded in the user data of the user database 31. If the received access request is one from any of the registered users, the CPU 21 accepts the access request.

Ex. 1007, ¶ [0095] (emphasis added).

275. A POSITA reading this passage understands that *Takahashi*’s use of the word “or” means the user may login with (1) user ID and password or (2) identification information. A POSITA also understands that the user ID and password is not specific to a device, which corresponds to revised amended claim 26[c]. Whether *Takahashi* also teaches using “a serial number of the mobile terminal” (Ex. 1007, ¶ [0074]) does not change *Takahashi*’s teaching that the user may “us[e] application specific authentication information that is not authentication information specific to a device,” i.e., a user ID and password. Additionally,

Takahashi discloses that “[i]dentification information is used mainly for user authentication that is executed after the mobile terminal 10 of a user accesses to the game server 20.” Ex. 1007, ¶ [0074]. A POSITA understands from this passage (and form ¶ [0095]) that a user ID and password is used for authenticating the initial access to the game server, and that the identification information may be used in subsequent accesses after the device is registered (e.g., serial number information stored in the “Identification Information” column shown in *Takahashi* Figure 6).

User ID	Password	Identification Information	Terminal information of main-terminal	Terminal information of sub-terminal
012345	knm001	xxxxxxxxxx		

Ex. 1007, Fig. 6. The existence of this additional authentication method does not change the fact that the user ID and password are not specific to a device.

276. Patent Owner and its expert make an argument that the Board’s Preliminary Guidance incorrectly suggests it would be reasonable to combine

Takahashi with *Kling*'s multiple/different passwords to improve *Takahashi*'s security against malware. RMTA at 20-21; Ex. 2008 ¶¶ 138-40. In particular, Patent Owner argues, both *Takahashi* with *Kling* disclose using device specific authentication information. *Id.* I disagree. As described above, both *Takahashi* and *Kling* disclose using identification/password credentials to login on both a personal computer and a mobile phone. Password credentials are not specific to a device. Regardless, Petitioner's grounds no longer expressly combine *Takahashi* with *Kling*. As discussed below, *Takahashi* is instead combined with *Gui*'s teaching of different passwords for the different devices.

3. Revised substitute claim 27

277. For revised substitute claim 27, Patent Owner and its expert argue 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; Ex. 2008 ¶¶ 144-46. I disagree for the reasons provided in my first declaration, namely, *Takahashi*'s game server sends the same fish object image data to both the main-terminal and the sub-terminal. Ex. 1002-164-67 at ¶¶ 256-260.

4. Revised substitute claim 28

278. For revised substitute claim 28, Patent Owner and its expert argue that "[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; Ex. 2008

¶¶ 151-53. As explained above, it is my opinion that revised substitute claim 28 lacks written description support. In addition, I disagree with Patent Owner's arguments for the reasons provided in my first declaration. Ex. 1002-167-69 at ¶¶261-263.

279. I also disagree with Patent Owner's argument because it ignores that *Takahashi* discloses playing a game with two devices from start to finish. As I discussed in my first declaration, this embodiment expressly teaches the limitations found in revised substitute claim 28. Indeed, Patent Owner'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.

5. *Zha* and *Takahashi* are “analogous”

280. Patent Owner argues *Zha* and *Takahashi* are not “analogous” prior art because “Dr. Rubin has modified the claims to specify all the Substitute Claims are explicitly directed toward enhancing information security.” RMTA at 24-25. However, I agree with the Board's Preliminary Guidance and believe it is correct:

Takahashi is in the same field of endeavor as the claimed invention because it also relates to 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.’ Ex. 1001, 2:29-31. Based on the current record, we are also persuaded by Petitioner's argument that Patent Owner is wrong to assert that the prior art must address the same problem as the '376 Patent.

PG at 24-25.

281. For revised amended claims 26 and 41, Patent Owner has amended the preambles to recite “protecting information” and added “thereby” clauses reciting “protecting . . . from potential malware.” However, I understand the Board’s Preliminary Guidance indicates it is wrong to assert the prior art must address the same problem as the ’376 Patent. Thus, in my opinion, *Zha* and *Takahashi* are in the same field of endeavor as the revised claims because they both relate to systems or methods in which a user interacts with a first electronic device and a second electronic device throughout the use of an online application.

XIII. ADDITIONAL GROUNDS: *TAKAHASHI* GROUNDS COMBINED WITH *GUI*

282. In my declaration submitted in support of the Petition (Ex. 1002), I provided my opinion that claims 1-5, 9-10, 12-14, 16-17, and 23-25 are unpatentable based on the *Takahashi* Grounds along with the POSITA’s knowledge and/or other prior art references. *See* Ex. 1002 ¶ 50 (Grounds 7-8).

283. It is my opinion a POSITA would be motivated to combine *Gui* with the other prior art (Grounds 7-8) for the same reasons I provide above in Section X.A, which I incorporate herein by reference. Consequently, it is my opinion that substitute claims 26-35 and 37-41 are unpatentable based on the *Takahashi* Grounds as modified by *Gui*’s disclosure of using multiple/different passwords with different devices.

284. This combination uses *Gui*'s teaching of why an application might use different passwords for different devices to render the revised substitute claims obvious in view of *Takahashi* and *Gui*. This combination does not require the full implementation of *Gui*'s distributed credential system (e.g., *Gui* Figure 3) in combination with *Takahashi*. In other words, a POSITA would simply modify *Takahashi* so that the game application allows different passwords to access the same user account, for the reasons taught by *Gui*. *Takahashi*'s game application would handle the device authentication just as *Gui* Figure 2 shows the service (i.e., the application) handling the device authentication:

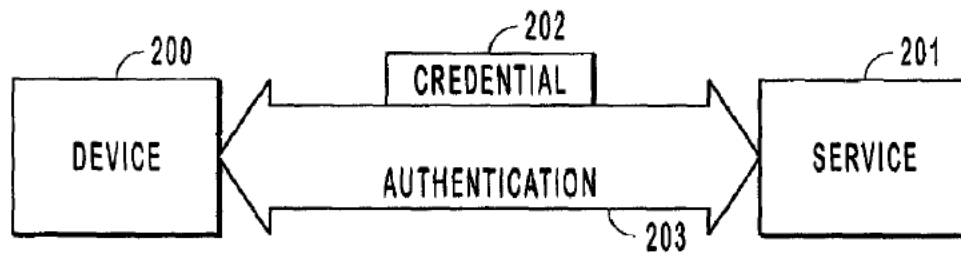


FIG. 2

Ex. 1031, Fig. 2.

285. I discuss above for the *Zha/Gui* grounds *Gui*'s teaching of different passwords for different devices, and that discussion applies equally here.

286. Thus, it is my opinion that a POSITA would have found the use of different application specific authentication information (e.g., passwords) for

accessing *Takahashi's* game application from a mobile phone versus from a desktop/laptop computer to be an obvious modification of *Takahashi*. 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).

287. It is my opinion that a POSITA would find modifying *Takahashi* with *Gui's* multiple passwords to be a trivial and, thus, would have a reasonable expectation of success. In fact, it is my opinion that *Takahashi* 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.

APPENDIX D1 – LIST OF MATERIALS CONSIDERED

Rubin, U.S. Patent No. 9,064,376 (“the ’376 Patent”)
Prosecution History File Wrapper of the ’376 Patent (excerpts)
U.S. Patent No. 9,497,565 (“*Zha*”)
CN 2013/10674692 (“*Zha Priority Application*”)
Certified English translation of the *Zha Priority Application*
U.S. Patent Pub. No. 2015/0011318 (“*Takahashi*”)
PCT/JP2012/007595 (“*Takahashi Priority Application*”)
Certified English translation of *Takahashi Priority Application*
U.S. Patent Pub. No. 2014/0006485 (“*Tsushima*”)
U.S. Patent No. 9,591,083 (“*Gumbula*”)
U.S. Patent Pub. No. 2012/0017236 (“*Stafford*”)
U.S. Patent No. 9,330,531 (“*Wakeford*”)
Patent Owner’s Preliminary Infringement Contentions in *Rubin v. Kahoot! ASA et al.*, Civil Action No. 6:22-cv-00236 (W.D. Tex.) (Sept. 28, 2022)
U.S. Patent Pub. No. 2012/0253841 (“’841 Application”)
U.S. Patent Pub. No. 2012/0209770 (“’770 Application”)
U.S. Patent Pub. No. 2014/0121015 (“*Massing*”)
U.S. Patent Pub. No. 2006/0058088 (“*Crawford*”)
Complaint (Dkt. 001) in *Rubin v. Kahoot! ASA et al.*, Civil Action No. 6:22-cv- 00236 (W.D. Tex.) (Sept. 28, 2022)
Answer (Dkt. 021) in *Rubin v. Kahoot! ASA et al.*, Civil Action No. 6:22-cv-00236 (W.D. Tex.) (Sept. 28, 2022)
U.S. Patent Pub. No. 2012/0240203 (“*Kling*”)
U.S. Patent Pub. No. 2014/0033292 (“*Moore*”)
U.S. Patent Pub. No. 2012/0222102 (“*Hirose*”)
U.S. Patent Pub. No. 2014/0189841 (“*Metke*”)
U.S. Patent Pub. No. 2013/0337916 (“*Saretto*”)
U.S. Patent No. 9,397,989 (“*Ramalingam*”)
Deposition Transcript of Patrick Traynor 02/15/2024 – Rough Draft

Deposition Transcript of Patrick Traynor 02/15/2024 – Official Full Size

Deposition Transcript of Patrick Traynor 02/15/2024 – Official Condensed

L. St. Clair *et al.*, “Password Exhaustion: Predicting the End of Password Usefulness,” ICISS 2006, LNCS 4332, pp. 37-55 (Springer-Verlag Berlin Hiedelberg 2006)

U.S. Patent No. 7,865,950 (“*Lipetz*”)

U.S. Patent Pub. No. 2013/0023241 (“*Lim*”)

U.S. Patent No. 7,676,829 (“*Gui*”)

Deposition Transcript of Patrick Traynor – May 13, 2024 (condensed)