

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

SECOND 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.

February 23, 2024

By:

A handwritten signature in blue ink, appearing to read 'S. Meldal', written over a horizontal line.

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)

LIST OF APPENDICES

Appendix D1 List of Materials Considered

TABLE OF CONTENTS

I.	INTRODUCTION	10
II.	PATENT OWNER’S LACK OF WRITTEN DESCRIPTION SUPPORT FOR CLAIM AMENDMENTS	10
A.	Legal Standard.	10
B.	The term “application specific authentication information,” as it is used in the substitute claims and by Patent Owner and its expert, is not described in the cited portions of the ’376 Patent specification.....	11
C.	The phrase “providing a notification by the application on the second device that the connectivity has been disrupted” in substitute claim 30 is not described in the cited portions of the ’995 App.....	25
D.	The limitations directed to “wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device” lack support.	28
III.	THE MEANINGS OF “APPLICATION SPECIFIC AUTHENTICATION INFORMATION” AND “PROVIDING A NOTIFICATION BY THE APPLICATION ON THE SECOND DEVICE” FAIL TO INFORM A POSITA ABOUT THE SCOPE OF THE INVENTION	28
A.	Legal Standard.	28
B.	Newly Added Phrases Fail to Inform a POSITA About Their Scope.....	28
IV.	CLAIM CONSTRUCTION	31
A.	Legal Standard	31
B.	Patent Owner does not construe “application specific authentication information.”	33
C.	Patent Owner’s Construction of “sensitive information”	33
V.	INFORMATION CONSIDERED	34

VI. THE SUBSTITUTE CLAIMS 26-41 ARE INVALID IN VIEW OF PRIOR ART.....	35
A. Legal Standard of Obviousness	35
B. Level of Ordinary Skill in the Art.....	37
VII. OVERVIEW OF CONCLUSIONS	40
VIII. RECITATION OF THE SUBSTITUTE CLAIMS	42
IX. GROUND 9: SUBSTITUTE CLAIMS 26-29, 31, 34, AND 40-41 ARE OBVIOUS OVER <i>KLING</i> AND A POSITA’S GENERAL KNOWLEDGE.....	46
A. Overview of <i>Kling</i>	46
B. Independent Substitute Claim 26.....	53
1. [26Preamble] “A method for transmitting information to multiple electronic devices, the method comprising:”	53
2. [26a] “electronically storing a set of information at a server,”	54
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;”	55
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 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;”	63
5. [26d] “if and only if both the first and second devices are determined to be accessible by the server, then:”	

	<i>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.”</i>	70
C.	Substitute Claim 27 — “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.”	79
D.	Substitute Claim 28 — “the first subset of the information comprises <i>non-sensitive information</i> ; and the second subset of the information comprises sensitive information”	81
E.	Substitute Claim 29 — “wherein the information received at the second device is more sensitive than the information received at the first device”	82
F.	Substitute Claim 31 — “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.”	83
G.	Substitute Claim 34 — “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”	85
H.	Substitute Claim 40 — “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.”	91
I.	Independent Substitute Claim 41	92
1.	<i>[41Preamble] “A system for transmitting information to multiple electronic devices, the system comprising:”</i>	92
2.	<i>[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</i>	

	<i>generated by the same application at the server and are specific to that application”</i>	93
3.	<i>[41b] “a processor device programmed for:”</i>	100
4.	<i>[41c] “identifying a first subset of the information and identifying a second subset of the information;”</i>	100
5.	<i>[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 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;”</i>	100
6.	<i>[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.”</i>	101
X.	THE PETITION GROUNDS WITH ZHA AS PRIMARY REFERENCE	101
A.	Obviousness under 35 U.S.C. § 103	101
1.	<i>Substitute Claims 26 and 41</i>	101
2.	<i>Substitute Claims 27-29, 31-34, and 36-40</i>	108
3.	<i>Substitute Claim 30</i>	108
4.	<i>Substitute Claim 35</i>	111
B.	Response to Patent Owner’s Arguments Related to Zha Grounds	113

1.	<i>“authentication information”</i>	113
2.	<i>“sensitive information”</i>	114
3.	<i>“sensitive information” (i) generated by the application (ii) at the server and (iii) specific to the application</i>	116
4.	<i>Motivation to combine Zha with POSITA’s knowledge, Tsushima and “analogous” art</i>	118
XI.	ADDITIONAL GROUNDS: ZHA GROUNDS COMBINED WITH KLING	123
XII.	THE PETITION GROUNDS WITH TAKAHASHI AS PRIMARY REFERENCE	123
A.	Obviousness under 35 U.S.C. § 103	123
1.	<i>Substitute Claims 26 and 41</i>	124
2.	<i>Substitute Claims 27-29, 31-34, and 37-41</i>	132
3.	<i>Substitute Claim 30</i>	132
4.	<i>Substitute Claim 35</i>	134
B.	Response to Patent Owner’s Arguments Related to <i>Takahashi</i> Grounds	135
1.	<i>Login process followed by an authentication process</i>	135
2.	<i>“sensitive information”</i>	137
3.	<i>Motivation to combine Takahashi with POSITA’s knowledge, Tsushima; Prior art is “analogous”</i>	141
XIII.	ADDITIONAL GROUNDS: TAKAHASHI GROUNDS COMBINED WITH KLING	143

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. I have been asked to provide my opinion about: (1) whether the '376 Patent specification provides a written description under 35 U.S.C. § 112 for Patent Owner's proposed claim amendments, including for (a) new term "application specific authentication information" (substitute claims 26 and 41) and (b) "providing a notification by the application on the second device that the connectivity has been disrupted" (substitute claim 30) (collectively, the "New Limitations"); (2) whether, for purposes of definiteness under 35 U.S.C. § 112, the New Limitations contain words or phrases 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; (3) the proper claim construction of the term "sensitive information"; and (4) whether substitute claims 26-41 are patentable in view of the prior art.

II. PATENT OWNER'S LACK OF WRITTEN DESCRIPTION SUPPORT FOR CLAIM AMENDMENTS

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. The term “application specific authentication information,” as it is used in the substitute claims and by Patent Owner and its expert, is not described in the cited portions of the '376 Patent specification.

4. Accordingly, my opinion related to the written description evaluates Patent Owner's identification and explanation of alleged support for the amended/substitute claims. I reserve the right to supplement this declaration should Patent Owner be allowed to provide further explanation and/or identify further support for the amended/substitute claims.

5. Patent Owner seeks to amend substitute claims 26 and 41 to recite “application specific authentication information.” I note that the '376 Patent does not use this term.

6. Neither Patent Owner nor its expert, Dr. Traynor, have offered a claim construction for the term “application specific authentication information.” Counsel has informed me that it is Patent Owner's burden to justify the substitute claims. Therefore, I have not proposed a claim construction for the term in the first instance. My analysis of the written description support (i.e., lack of support) for the new term is based on the current record and Patent Owner's apparent understanding of the term. Patent Owner's failure to provide a succinct definition of this newly-coined

term is prejudicial to my analysis because I am forced to guess at what Patent Owner believes the scope of the term 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. Substitute claims 26 and 41 recite “a set of information at a server” ([26a], [41a]) where “subsets of information are generated by the same application at the server” ([26b], [41a]). The amendments to substitute claims 26 and 41 recite “determining **at the server** ... based on the first user being logged into **the application** using application specific authentication information...” ([26c], [41d] (emphasis added)). Based on this new claim language, a person of ordinary skill in the art would understand that the “application specific authentication information” is related to “the same application at the server.” Accordingly, it is my understanding that it is Patent Owner’s burden to show written description support for the new amendment as it is used in the amended/substitute claims.

8. Patent Owner identifies Figure 10 and paragraphs 26, 33, 75, 83, 89, 90, and 92 of U.S. Patent Application No. 14/444,995 (“the ’995 App.”) as alleged support for amended/substitute claim limitations, i.e., limitations [26c] and [41d], that recite “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.”

9. I note that Patent Owner has not explained how any of the cited portions of the '995 App. actually support the amended claim limitations. 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, in particular in light of how Patent Owner has apparently construed the term “application specific authentication information.” Based on my review of those cited portions, it is my opinion that the disclosure of those portions does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter as of the filing date.

10. Patent Owner cites ¶ 26 of the '995 App.:

[26] In one example of a preferred embodiment, illustrated in Fig. 2, a user is playing online poker, and the user sees the same view of a table as is common in online poker, but the hole cards are not displayed (210). In this embodiment, the user runs a separate app on a second device (215) that uses its own authentication (which can be different from the authentication required on the first device), and over that channel, the game server sends the user the hole cards for that hand. An identifier is used to link the current hand on the first device to the hole cards that are displayed on the second device.

Ex. 2005-006.

11. This passage (¶ 26) does not provide support for “application specific authentication information” in substitute claims 26 and 41 because, at best, it discusses authentication by a separate application running on the second device. In

contrast, the amendments to substitute claims 26 and 41 relate to “application specific authentication information” for “the same application at the server” (as I discuss above). In other words, the authentication information in the substitute claims appears to be specific to “the same application at the server,” whereas the authentication information discussed in ¶ 26 relates to application software running on the individual device – not “at the server.” Thus, it is my opinion that ¶ 26 of the ’995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application specific authentication information” for “the same application at the server”) as of the filing date.

12. Patent Owner cites ¶ 33 of the ’995 App.:

[33] In some embodiments, the server can be configured to determine whether both a first device and a second device are accessible over at least one electronic communications network. According to one embodiment, the server maintains a heartbeat message with the second device. This can be a simple ping message (*e.g.*, via ICMP) or a short message over an existing TCP/IP connection. In some embodiments, the determination of accessibility can be made by transmitting arbitrary packets over a TCP connection and receiving an acknowledgment and inaccessibility determined by the absence of an acknowledgement. In this manner, the server can determine the status and availability of the second device. In the event that there is a network connection disruption with the second device, the server may attempt to switch communication mechanisms to use text message instead of the Internet. Alternatively or in addition, the server may terminate the session.

Ex. 2005-008.

13. This passage (¶ 33) does not provide support for “application specific

authentication information” in substitute claims 26 and 41. This passage appears to relate to monitoring connectivity using a heartbeat message, and a person of ordinary skill in the art would not understand that to be “application specific authentication information” or provide support for that new term. Thus, it is my opinion that ¶ 33 of the ’995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application specific authentication information” for “the same application at the server”) as of the filing date.

14. Patent Owner cites ¶ 75 and Figure 10 of the ’995 App.:

[75] Fig. 10 illustrates an example of a database entry on the central server for a particular user in the banking example. The central server can store hashes of the passwords that are used on the first device and the second device. When a user submits a password on a device, the device hashes the password and sends the hash to the central server over a secure connection

(e.g., SSL). The central server extracts the stored password from the database shown in the figure and compares the two. If they match, then authentication is successful. The figure shows that the database may store the authentication token as described above, as well as information about the user’s preferences, such as the dollar amount above which use of a second device is required for funds transfers.

Ex. 2005-017 to -018.

username	John Doe
requires second device	Yes
hashed pw for first device	3987a87b87c73f3490c9d0
hashed pw for second device	98b7c73a347e789f98d342
authentication token	98234f342e324a7cd98b2a
funds transfer threshold	\$800
link to bank account info	Pointer to banking database: 0x00123adf32 Key to user entry in bank database: 3a98c3243f

Example database entry on central server
for user John Doe in banking example

Ex. 2005-043.

15. These portions (§ 75 and Figure 10) do not provide support for “application specific authentication information” in substitute claims 26 can 41 because, at best, they discuss authentication by two passwords but do not disclose how those passwords are “application specific.” In addition, during his deposition, Patent Owner’s expert, Dr. Traynor, distinguished authentication used by *Tsushima*’s server as not disclosing “application specific authentication information” because authentication information for the server (i.e., where the server

performs the authentication) is allegedly not the same as authentication information for the application (i.e., is not “application specific”). If Dr. Traynor is correct, the same rationale would reasonably apply to these portions (§ 75 and Figure 10) because the authentication is being performed by “[t]he central server” and not an application.

16. Additionally, these portions (§ 75 and Figure 10) do not disclose “application specific authentication information” under Patent Owner’s apparent construction of the term in a way that excludes “device specific” information. Tellingly, neither Patent Owner nor its expert explain what is and is not “device specific”—they just argue that device specific information is not application specific. This issue is further confused by Dr. Traynor’s admission during deposition that “device specific” information may be used as part of “application specific authentication information.” Ex. 1026, 127:20-128:14, 130:17-131:19. In addition, Dr. Traynor suggested that whether device specific information could be application specific information depends on whether the information was provided by the manufacturer as opposed to a user or the system or something else. Ex. 1026, 126:2-128:20. Dr. Traynor’s testimony about what is and is not “application specific authentication information” is not supported by the patent specification (or the plain meaning) and further confuses the issue of determining the scope of this newly coined term and whether the term has written description support.

17. As depicted in Figure 10, one password is assigned to the “first device” and the second password is assigned to the “second device.” Thus, each password is device specific under Patent Owner’s reasoning, as it is tied to a specific device. For example, based on these portions (§ 75 and Figure 10), one of ordinary skill in the art would understand the first listed password (“hashed pw for first device”) is used to authenticate the user’s first device and the second listed password (“hashed pw for the second device”) is used to authenticate the user’s second device. Figure 10 shows a field “requires second device” is set to “Yes,” thus a person of ordinary skill in the art would understand that the disclosed authentication mechanism (in this case for a banking application) would require the use of the second password by the second device before information can be sent to the second device. One of ordinary skill in the art would understand this second password is specific to the second device, or “device specific” under Patent Owner’s reasoning. Patent Owner and its expert have argued that the *Takahashi*’s prior art disclosure of “device specific” authentication information is not a disclosure of “application specific authentication information.” See Motion to Amend at 17 (“This is device specific authentication information, not application specific authentication information.”); Declaration of Patrick Traynor at 41 (§ 93) (“[*Takahashi*’s] ‘identification information’ is authentication that is specific to the device. Meaning it is authentication information that is not ‘application specific,’ but device specific.”). For at least these reasons, it

is my opinion that ¶ 75 and Figure 10 of the '995 App. do not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application specific authentication information” for “the same application at the server”) as of the filing date.

18. Patent Owner cites ¶ 83 of the '995 App.:

[83] The custom second device can optionally be initialized with security keys and cryptographic tokens, allowing the second device authentication capabilities, in addition to or instead of authentication by the user. For example, the device can be loaded with client SSL private keys and certificates, allowing the server to directly authenticate the custom second device. Additionally, user authentication inside of an application can allow for even greater

security. Since the custom second device may be much less vulnerable to malware than a standard computer, tablet or smartphone, these pre-loaded keys and cryptographic tokens are correspondingly less vulnerable to malware infections.

Ex. 2005-019 to -020.

19. This passage (¶ 83) does not provide support for “application specific authentication information” in substitute claims 26 and 41 under Patent Owner’s apparent construction of the term in a way that excludes “device specific” information. A person of ordinary skill in the art would understand the information used for authentication in this passage (security keys and cryptographic tokens) are specific to the second device. Indeed, ¶ 92 of the '995 App. specifically indicates that “if an authentication token is used on the second device, then the user will be limited to using that specific device whenever using the application with the central

server.” *See also* ’995 App. ¶ 90 (“any device without the authentication token cannot act as the second device”). This confirms the “device specific” nature of the disclosed security token. As explained in the paragraphs above, Patent Owner has distinguished “device specific” authentication information from “application specific” authentication information. Based on Patent Owner’s reasoning, the security keys and cryptographic tokens in ¶ 83 would be specific to the second device and, thus, do not provide support for the new term “application specific authentication information” under Patent Owner’s apparent construction of that term. Thus, it is my opinion that ¶ 83 of the ’995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application specific authentication information” for “the same application at the server”) as of the filing date.

20. Patent Owner cites ¶ 89 of the ’995 App.:

[89] At registration time, upon receiving a request to add a second device from a user's first device, the central server creates a new database entry or adds fields to an existing database record for the user for storing information about the user's second device. Next, in this example, the user initiates a connection to the central server from the second device, and the central server correlates the communication from the second device with the database entry created or modified based on earlier communication with the first device. In this embodiment, the central server creates authentication information, such as a 256-bit random number and sends that authentication information to the first device. Upon registering the second device, the user enters the authentication information into the second device to complete the registration. The authentication information, consisting of a 256 bit random string, in this example, can be converted into a human readable ASCII string using, for example, uuencoding, such that the user can read it and enter it into the second device. The central server uses the authentication information to ensure that only the actual user adds a new device, and that the new device that is added is added to the account of the correct user.

Ex. 2005-021.

21. This passage (§ 89) does not provide support for “application specific authentication information” in substitute claims 26 and 41. Rather, this passage describes registering the second device with the application “at registration time” by communicating a random number for use by the second device (“the user can read [the random number] and enter it into the second device”). One of ordinary skill in the art would understand the random number is specific to the registration of the second device. In other words, the random number is “device specific” because it can only be used to register the second device (not the first device). As explained in the paragraphs above, Patent Owner has distinguished “device specific” authentication information from “application specific” authentication information.

Based on Patent Owner's reasoning, the random number in ¶ 89 would be specific to the second device and, thus, does not provide support for the new term "application specific authentication information" under Patent Owner's apparent construction of that term.

22. Additionally, the random number in this passage (¶ 89) is used for purposes of registering the second device. In contrast, the "application specific authentication information" in substitute claims 26 and 41 related to "determining at the server ... based on the first user being logged into the application using application specific authentication information at both the first and second devices..." ([26c], [41d]). Thus, the "application specific authentication information" in the amended/substitute claims relates to logging in whereas this passage relates to registration of the second device. This is another reason why a person of ordinary skill in the art would not understand this passage (¶ 89) to provide support for "application specific authentication information," as used in the substitute claims.

23. For at least the reasons above, it is my opinion that ¶ 89 of the '995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., "application specific authentication information" for "the same application at the server") as of the filing date.

24. Patent Owner cites ¶ 90 of the '995 App.:

[90] If the first device is compromised by malware, then the attacker controlling the malware can learn the user's password. If the same authentication means is used for both devices, then the attacker could conceivably connect to the server with an illegitimate second device and impersonate the user. In some embodiments, the central server stores two different means of authenticating the user. One means of authentication, in some cases a password, is stored for authenticating the user on the first device, and a second means of authentication, possibly a different password, is stored to authenticate the user on the second device. Thus, two separate authentications can be used to prevent some attacks. In another embodiment, the central server and the second device can agree on a secret value, such as an authentication token, that is stored on the second device and in the central server database. Whenever the second device

communicates with the central server, the authentication token is used, such that any device without the authentication token cannot act as the second device.

Ex. 2005-021 to -022.

25. This passage (¶ 90) does not provide support for “application specific authentication information” in substitute claims 26 and 41 for the same reasons as I discuss above. In particular, this passage repeats (1) the two-password scenario I discuss above with respect to ¶ 75 and Figure 10 of the '995 App. and (2) the token scenario I discuss above with respect to ¶ 83 of the '995 App. In sum, both the two-password scenario and token scenario present “device specific” authentication information as Patent Owner has made that distinction. Thus, it is my opinion that ¶ 90 of the '995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application

specific authentication information” for “the same application at the server”) as of the filing date.

26. Patent Owner cites ¶ 92 of the '995 App.:

[92] It should be noted that if an authentication token is used on the second device, then the user will be limited to using that specific device whenever using the application with the central server. If it is desired to be able to use different devices to serve as the second device in the application, then the authentication should be limited to the user entering authentication information, such as a password, into the second device, which can then be any device that contains the appropriate application software.

Ex. 2005-022.

27. This passage (¶ 92) does not provide support for “application specific authentication information” in substitute claims 26 and 41. The passage first discusses use of an authentication token that is specific to the second device. I have already discussed (above with respect to ¶ 83) why the device-specific authentication token is not “application specific authentication information” based on Patent Owner’s distinction of “device specific” information. Additionally, while this passage discloses two passwords that can be used for authenticating “any device,” the passage is clear that the device itself must “contain[] the appropriate application software.” At best, this passage discusses authentication by a separate application running on the second device. In contrast, the amendments to substitute claims 26 and 41 relate to “application specific authentication information” for “the same application at the server” (as I discuss above). In other words, the authentication

information in the substitute claims appears to be specific to “the same application at the server,” whereas the authentication information discussed in ¶ 92 relates to application software running on the second device – not “at the server.” Thus, it is my opinion that ¶ 92 of the ’995 App. does not reasonably convey to persons of ordinary skill in the art that the inventor had possession of the claimed subject matter (i.e., “application specific authentication information” for “the same application at the server”) as of the filing date.

C. The phrase “providing a notification by the application on the second device that the connectivity has been disrupted” in substitute claim 30 is not described in the cited portions of the ’995 App.

28. Patent Owner seeks to amend substitute claim 30 to recite “providing a notification by the application on the second device that the connectivity has been disrupted” (underline emphasis is new limitation to previous claim). Patent Owner cites to ¶ 33 and original claim 5 of the ’995 App. as alleged support for amended/substitute claim limitation.

29. 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.

30. Initially, I note that “the application on the second device” lacks antecedent basis, as “an application on the second device” is not recited previously in substitute claim 30, or substitute claims 28 or 26, from which substitute claim 30 depends. Rather, substitute claim 26 recites an “application at the server.” A person of ordinary skill in the art would not understand this limitation to provide antecedent basis for the new amendment, “the application on the second device.”

31. Patent Owner cites ¶ 33 of the '995 App.:

[33] In some embodiments, the server can be configured to determine whether both a first device and a second device are accessible over at least one electronic communications network. According to one embodiment, the server maintains a heartbeat message with the second device. This can be a simple ping message (*e.g.*, via ICMP) or a short message over an existing TCP/IP connection. In some embodiments, the determination of accessibility can be made by transmitting arbitrary packets over a TCP connection and receiving an acknowledgment and inaccessibility determined by the absence of an acknowledgement. In this manner, the server can determine the status and availability of the second device. In the event that there is a network connection disruption with the second device, the server may attempt to switch communication mechanisms to use text message instead of the Internet. Alternatively or in addition, the server may terminate the session.

Ex. 2005-008.

32. This passage (¶ 33) does not provide support for “providing a notification by the application on the second device that the connectivity has been disrupted” in substitute claim 30. At most, this passage discloses the server switching communication mechanisms in the case of a network connection disruption, but does not disclose providing a notification. Moreover, this passage does not mention an “application on the second device” as it discusses the functionality of “the server.” The server taking the optional action of terminating the session does not disclose any particular action (or lack thereof) on the part of the application on the second device, much less the specific action of notifying on the second device that the connectivity has been disrupted.

33. Patent Owner cites original claim 5 of the '995 App.:

5. The method of claim 1, 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.

Ex. 2005-028.

34. While original claim 5 discloses providing a notification on the second device, it does not disclose doing so “by the application on the second device.”

35. For at least these reasons, it is my opinion that ¶ 33 and original claim 5 of the '995 App. do not reasonably convey to persons of ordinary skill in the art

that the inventor had possession of the claimed subject matter (i.e., “providing a notification by the application on the second device that the connectivity has been disrupted”) as of the filing date.

D. The limitations directed to “wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device” lack support.

36. This additional limitation in substitute claims 26 and 41 requires “the application specific authentication information.” As discussed above, Patent Owner has failed to show proper written description support for this term. This amendment is not supported for the same reasons.

III. THE MEANINGS OF “APPLICATION SPECIFIC AUTHENTICATION INFORMATION” AND “PROVIDING A NOTIFICATION BY THE APPLICATION ON THE SECOND DEVICE” FAIL TO INFORM A POSITA ABOUT THE SCOPE OF THE INVENTION

A. Legal Standard.

37. 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. Newly Added Phrases Fail to Inform a POSITA About Their Scope

38. In my opinion, a POSITA would find both phrases (a) “application specific authentication information” (substitute claims 26 and 41) and (b) “providing

a notification by the application on the second device that the connectivity has been disrupted” (substitute claim 30) do not inform a POSITA about their scope for the reasons discussed below.

39. Regarding the first new term, “application specific authentication information,” substitute claims 26 and 41 recite “a set of information at a server” ([26a], [41a]) where “subsets of information are generated by the same application at the server” ([26b], [41a]). The amendments to substitute claims 26 and 41 recite “determining **at the server** ... based on the first user being logged into **the application** using application specific authentication information...” ([26c], [41d] (emphasis added)). Based on this new claim language, a person of ordinary skill in the art would understand that the “application specific authentication information” is related to “the same application at the server.” During his deposition, Patent Owner’s expert, Dr. Traynor, distinguished *Tsushima*’s authentication from “application specific authentication information” because the user “appears to be logging into the server.” Ex. 1026, 106:8-14. According to Dr. Traynor, “the user appears to be logging into a service provision, a service” (Ex. 1026, 107:9-14), where the service performs the authentication. He testified, “there might be multiple applications running in this service. And so it’s not clear to me, because *Tsushima* mentions this in a very passing fashion what precisely the user is logging into.” Ex. 1026, 107:9-108:8. Thus, according to Dr. Traynor, “application specific

authentication information” does not include logging into a “service” that is running an application.

40. Additionally, Patent Owner apparently construes the term in a way that excludes “device specific” authentication information. MTA, Paper 19, pg. 17. In contrast, a POSITA would understand that device specific information could be application specific where the application actually requires and/or uses the information as part of its functionality. Neither Patent Owner nor its expert explain what is and is not “device specific”—they just argue that device specific information is not application specific. This issue is further confused by Dr. Traynor’s admission during deposition that device specific information may be used as part of “application specific authentication information.” Ex. 1026, 127:20-128:14, 130:17-131:19. In addition, Dr. Traynor suggested that whether device specific information could be application specific information depends on whether the information was provided by the manufacturer as opposed to a user or the system or something else. Ex. 1026, 125:14-123:16. Further compounding the issue, PO’s expert agrees that passwords, which are “user specific,” are also “application specific.” Ex. 1026, 72:4-9, 132:18-22. There is no reason why “device specific” information cannot also be “application specific” when “user specific” information can be. Both Patent Owner’s arguments and Dr. Traynor’s testimony about what is and is not “application specific authentication information” render the substitute claims unclear.

41. Regarding the second new term, “providing a notification **by the application** on the second device that the connectivity has been disrupted,” it is unclear whether the “the application” is on the server or on the second device. Substitute claim 30 is unclear because the newly added phrase “by the application” could refer to either “the application on the second device” (i.e., as written) or “the application” at the server. Which application is providing a notification is important to understanding the claim. Neither the specification nor the file history clarify this ambiguity.

IV. CLAIM CONSTRUCTION

A. Legal Standard

42. 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.

43. 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. Patent Owner does not construe “application specific authentication information.”

44. PO’s amended substitute claims 26 and 41 add a new term—“application specific authentication information.” PO does not provide a construction for this new term. *See* MTA, Paper 19, pgs. 8-10. PO’s expert witness, Dr. Traynor, testified the proper construction is plain and ordinary meaning. Ex. 1026, 69:5-10, 70:2-7.

45. However, it is my opinion that Dr. Traynor’s (and Patent Owner’s) analysis of this term with respect to the prior art is not based on a plain and ordinary claim construction. Rather, Patent Owner and Dr. Traynor appear to provide an overly narrow construction that excludes the prior art based on assertions that “device specific” authentication information cannot be “application specific.” While it is unclear what Dr. Traynor and Patent Owner believe to be the proper scope of this term, their overly narrow construction, as evident from their application of the term to the prior art, does not find support in the specification passages Dr. Traynor and Patent Owner cite as alleged support for the term (e.g., the passages discussed above in Section II.B).

C. Patent Owner’s Construction of “sensitive information”

46. PO and PO’s expert have proposed a construction of the term “sensitive information” to be “information that the application will not automatically share with the first device without first seeking the user’s permission.” In my opinion, this

construction is inconsistent with the plain meaning of the term to a person of ordinary skill in the art. Moreover, PO's proposed construction contradicts the specification where sensitive information is automatically shared with the first device when the second device is not present (Ex. 1001, 4:10-12).

47. PO's proposed construction is also in conflict with the use of the term in substitute claim 29, which recites "wherein the information received at the second device is **more sensitive** than the information received at the first device." Based on PO's proposed construction, substitute claim 29 would read:

The method of claim 26, wherein the information received at the second device is **more not automatically** shared with the first device without first seeking the user's permission than the information received at the first device.

48. PO's construction makes information sensitive or not, a binary classification, whereas substitute claim 29 requires degrees of sensitivity.

49. Thus, PO's construction should be rejected.

50. In my opinion, the plain meaning of "sensitive information" is the proper construction.

V. INFORMATION CONSIDERED

51. 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 and in the Petition.

52. 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.

53. 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 SUBSTITUTE CLAIMS 26-41 ARE INVALID IN VIEW OF PRIOR ART

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

A. Legal Standard of Obviousness

55. 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.

56. 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. 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.

57. 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.

58. 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.

59. 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

60. 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 computer and/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.

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

62. 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.

63. 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.

64. 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

65. I have reviewed and agree with the analysis in the Petitioner's Opposition to Motion to Amend. It is my opinion that each and every limitation of each and every 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 Motion to Amend and further explained in this declaration. Below is a summary of my conclusions:

- GROUND 9 – It is my opinion that substitute claims 26-29, 31, 34, and 40-41 are unpatentable in view of U.S. Publication No. 2012/0240203 (*Kling*) (Ex. 1023) and a POSITA's general knowledge.
- Petition Grounds 1-6 – It is my opinion that 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 *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 *Kling*'s disclosure of different passwords used as application specific authentication information for systems utilizing multiple devices where malware is a concern and sensitive information is to be protected.
- 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*, 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 *Kling*'s disclosure of different passwords used as application specific authentication information for systems utilizing multiple devices where malware is a concern and sensitive information is to be protected.

VIII. RECITATION OF THE SUBSTITUTE CLAIMS

Claim	Substitute Claim Language
26	[26Preamble] A method for 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</u>

	<u>authentication information</u> 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; [26d] 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.
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.
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 <u>by the application</u> 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 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> 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>; [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.

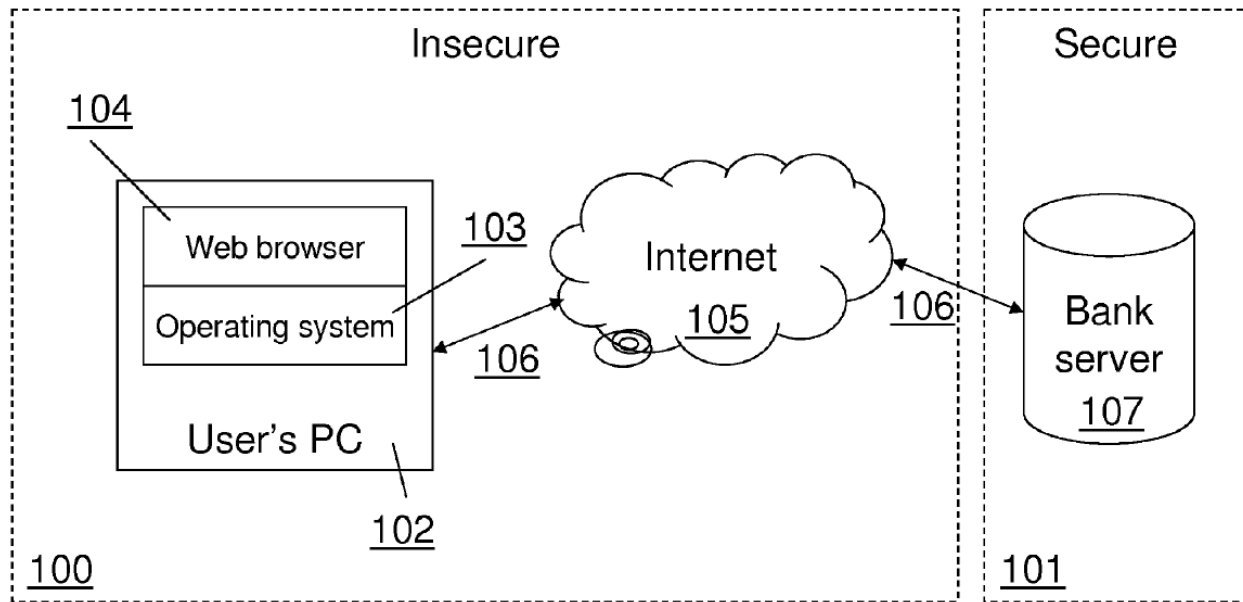
IX. GROUND 9: SUBSTITUTE CLAIMS 26-29, 31, 34, AND 40-41 ARE OBVIOUS OVER *KLING* AND A POSITA'S GENERAL KNOWLEDGE

A. Overview of *Kling*

66. 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).

67. *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].

68. “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].



69. 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]. 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 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.

70. 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.

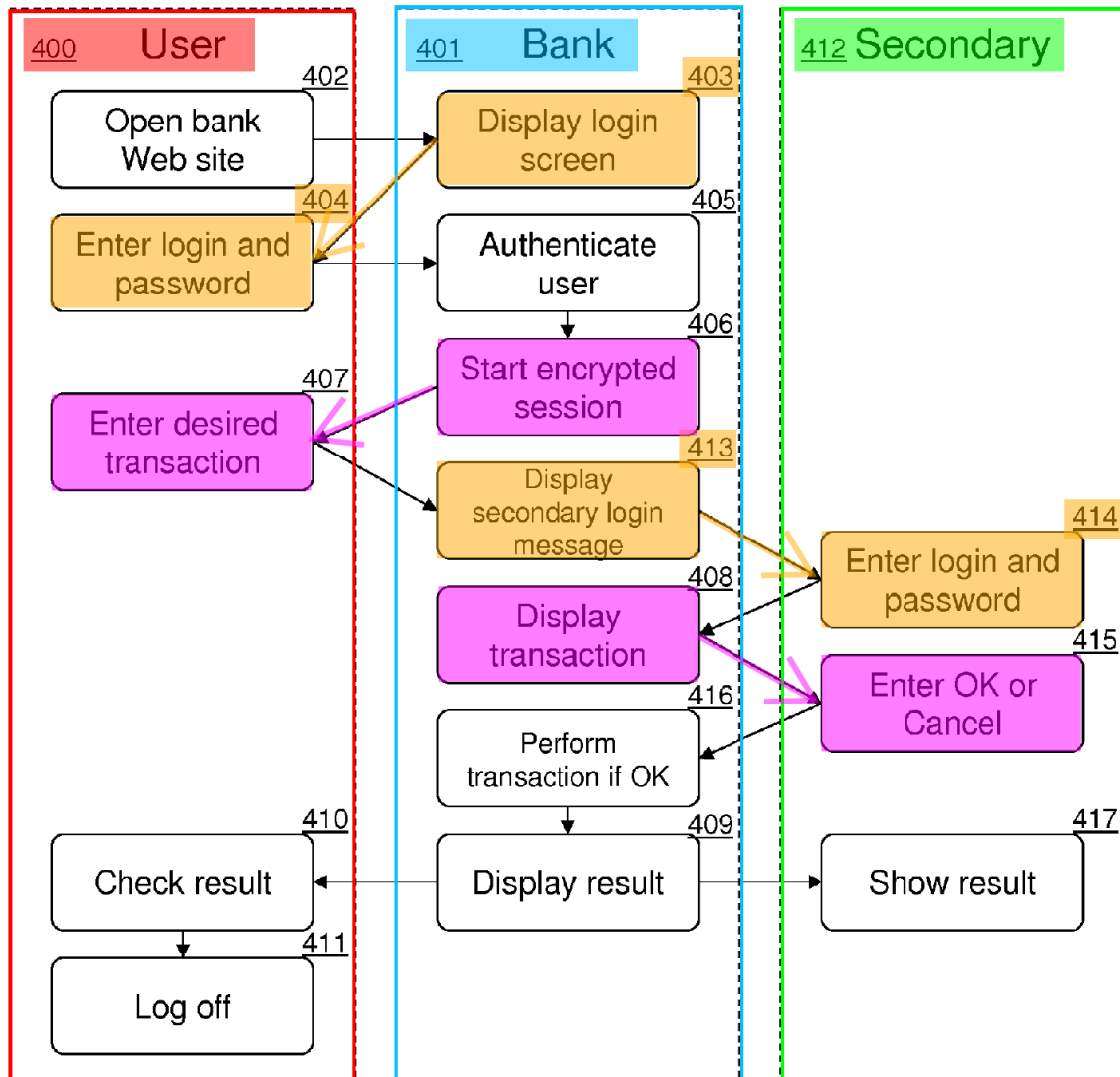


FIG. 4

71. 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.

72. “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].

73. 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.

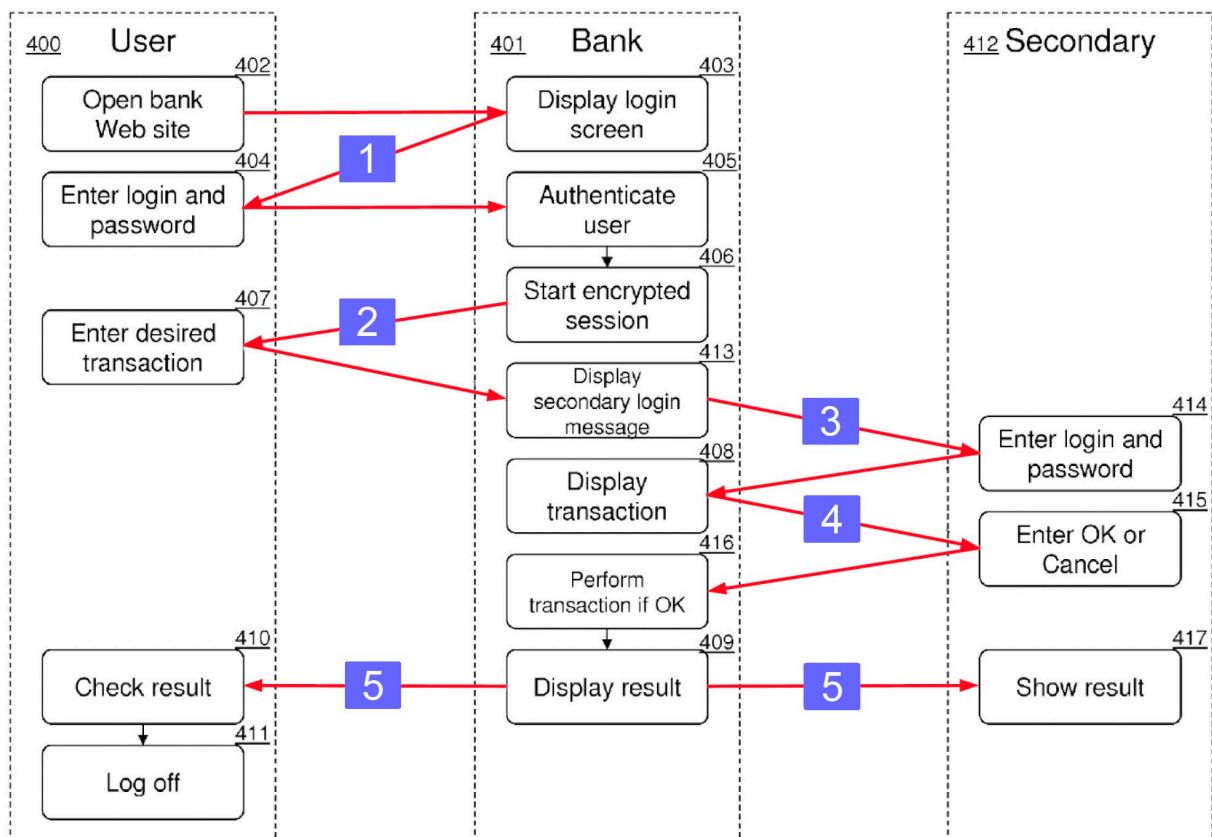


FIG. 4

- 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)

74. 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 form elements for entering a username and password ("Enter login and password" in box 404). Ex. 1023 ¶¶ [0017], [0014].

75. 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].

76. 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].

77. 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) form elements 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) and an identifier of the external account to which the money is to be transferred. *Id.*

78. 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. Independent Substitute Claim 26

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

79. To the extent the preamble is limiting, *Kling* discloses this element. *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].

80. 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.

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

81. *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.”

82. 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.

83. 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.

84. 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.

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 [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.

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;”

86. *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]; 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.”). 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].

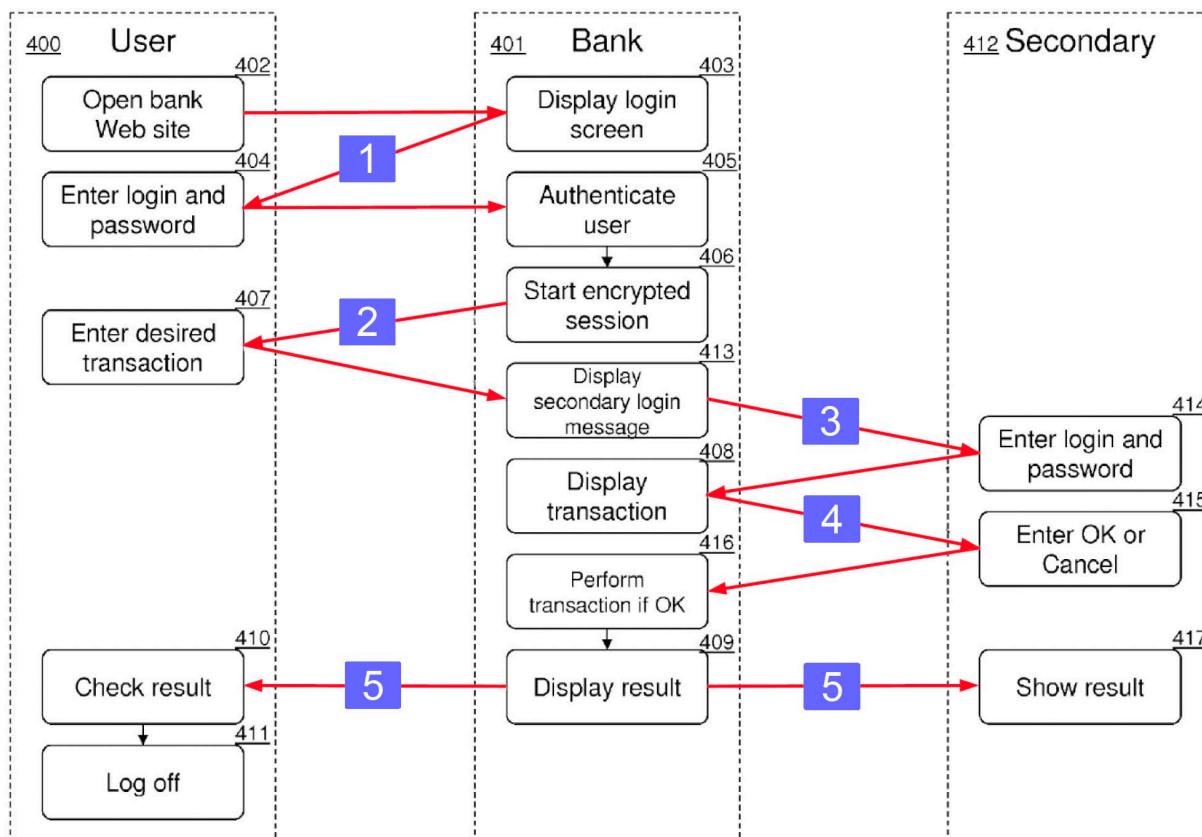


FIG. 4

- 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 (annotated).¹

87. 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

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

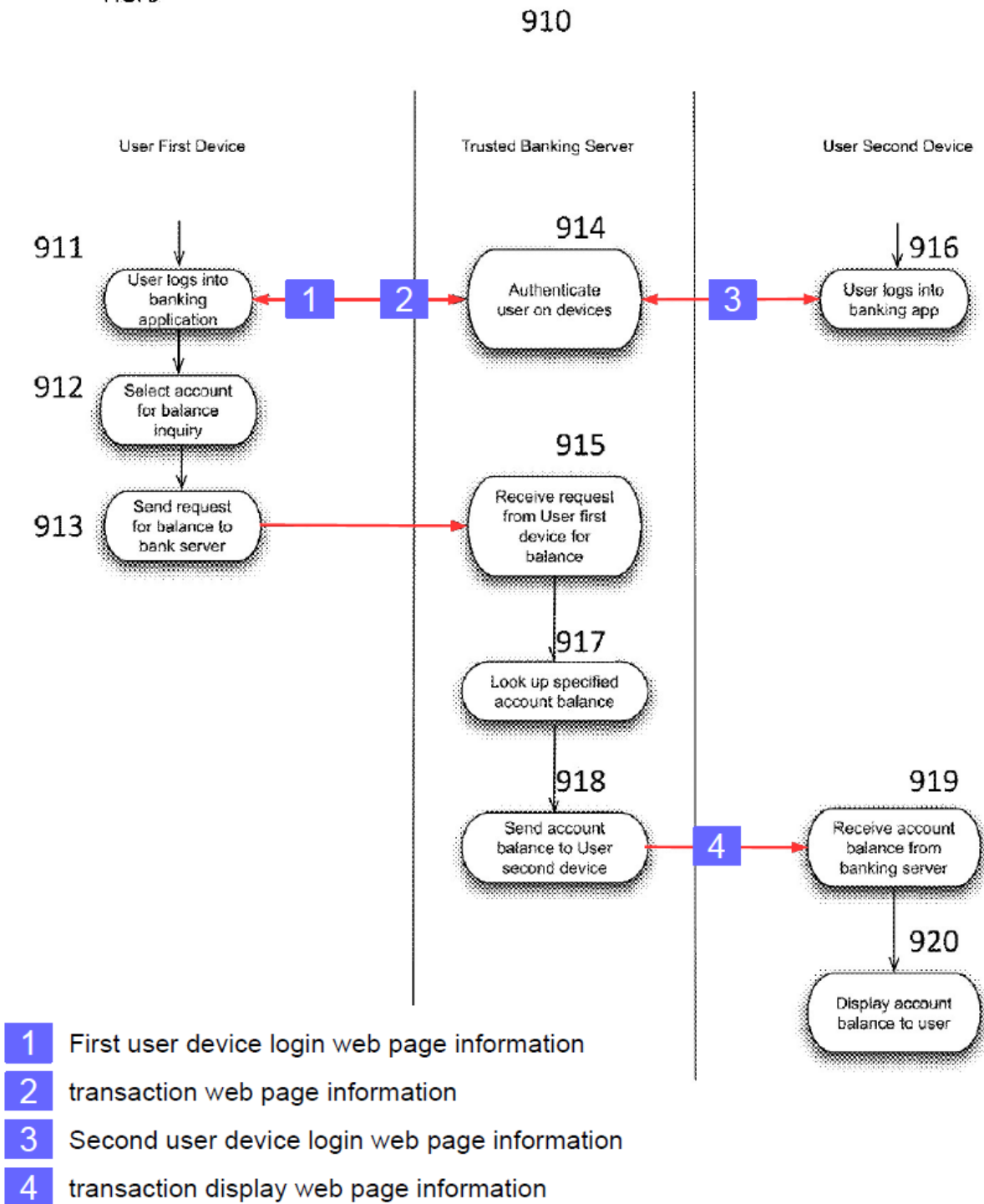
“first subset of information.” Second, the transaction confirmation web page information [Arrow #4] sent to the mobile device to display the transaction 408 and for the user to “enter OK or cancel” 415 corresponds to the claimed “second subset of information.” Both web pages for the PC “session” and the mobile device “session” are generated by server banking application (Web site 202) at the server 401 and are specific to the banking application.

88. 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.

89. 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

90. 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.

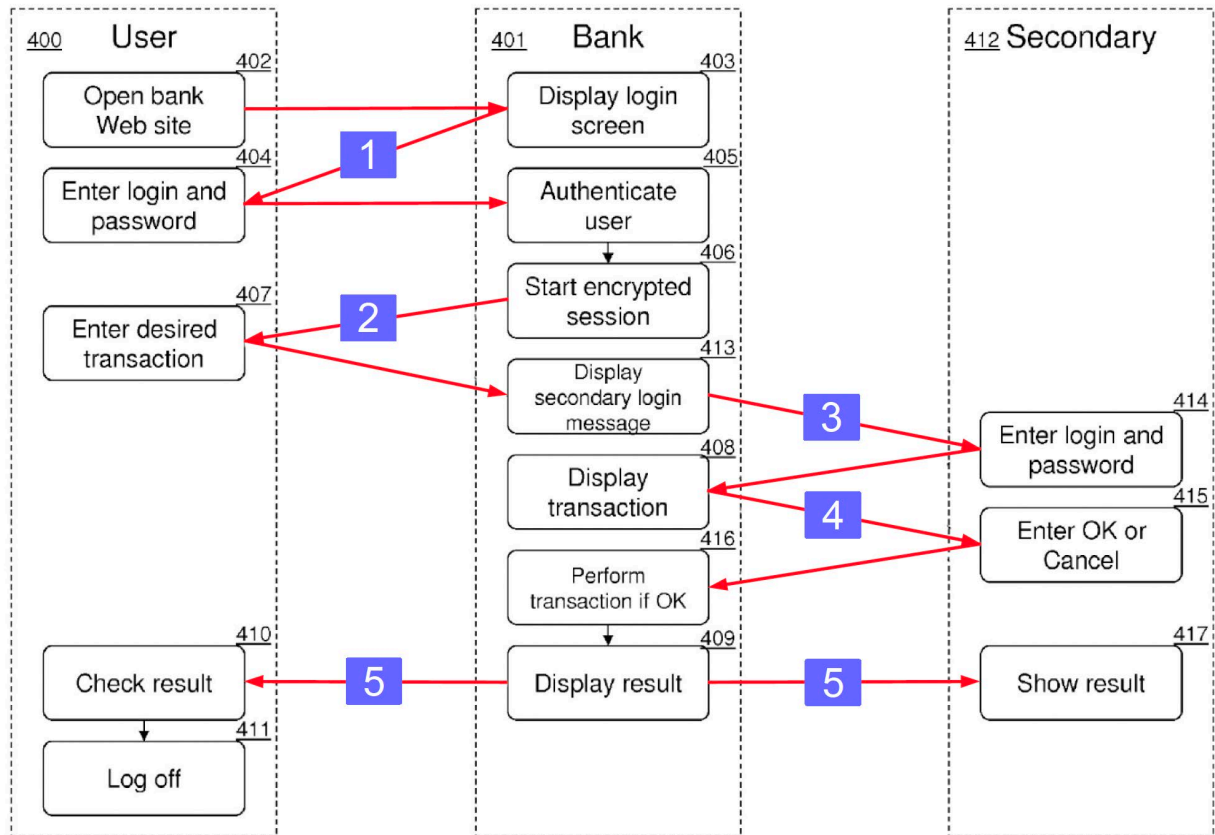


FIG. 4

- 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 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;”

91. As noted above, “application specific authentication information” is a new phrase not used in the ’376 Patent and Patent Owner has not provided a construction. Notwithstanding, *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.

92. In particular, *Kling* teaches, on a PC, “the user would open a Web site 2020, 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 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 412 after the user has "enter[ed] login and password" via the secondary 412 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 secondary 412 unless it had authenticated the user on the secondary 412. 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].

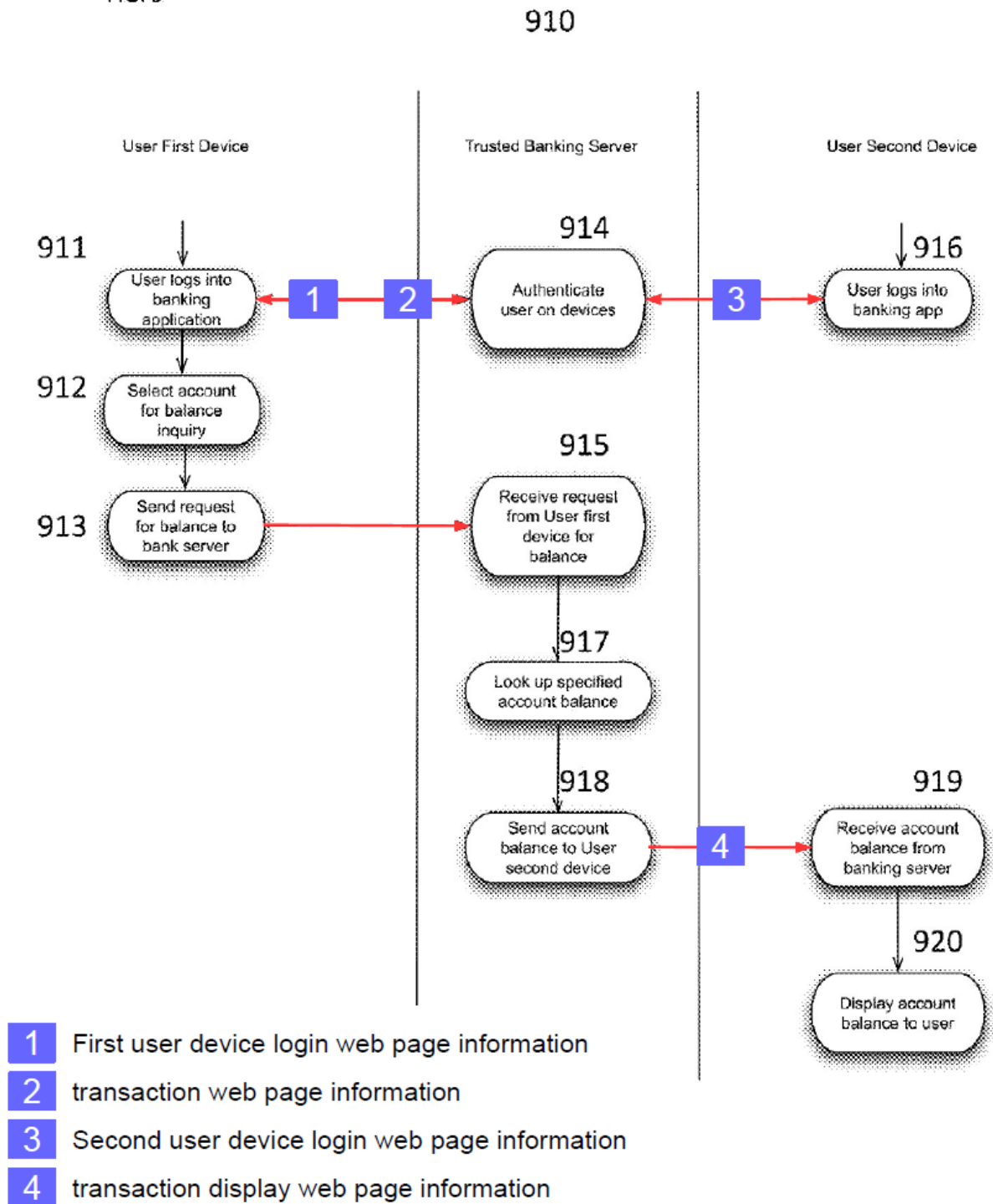
93. The *Kling* bank server 401 generates both the PC and mobile device web pages for the user to separately provide passwords to the same banking application, and the server 401 authenticates the passwords. Ex. 1023, Figure 4.

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.* 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.

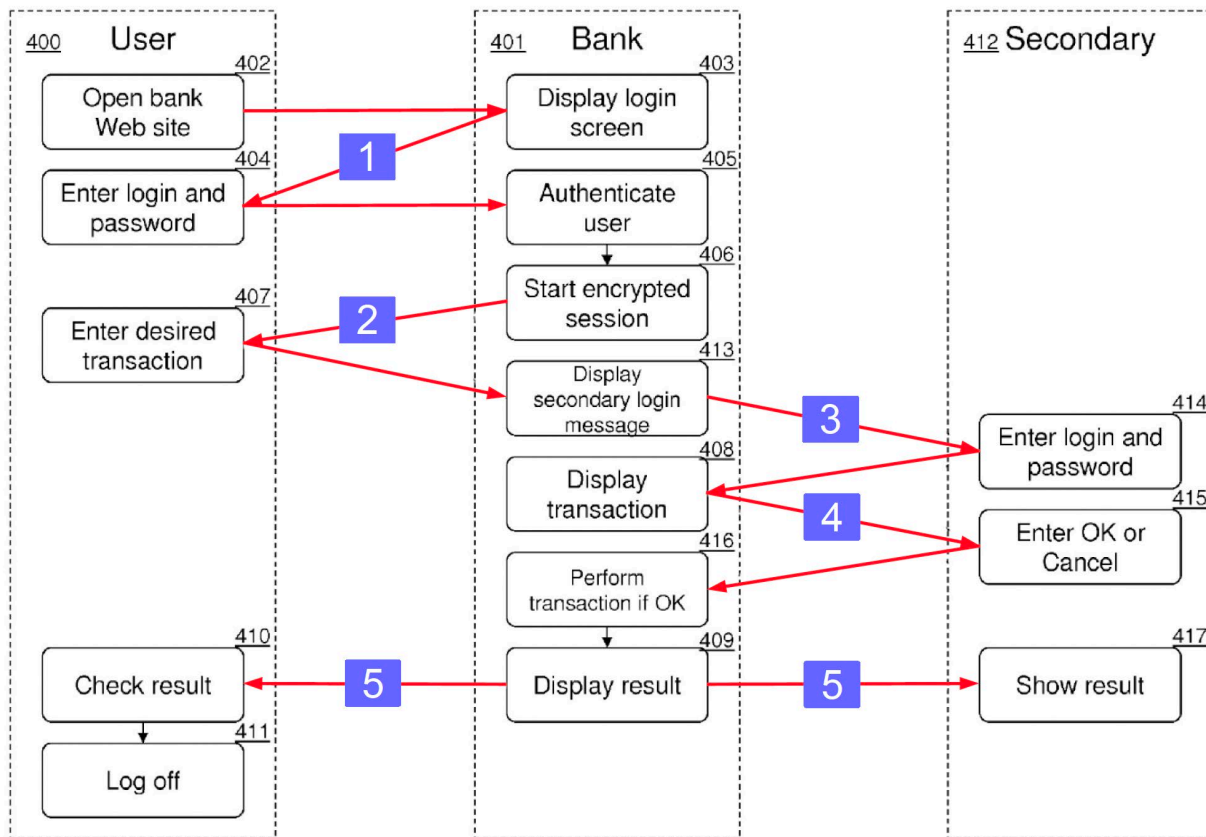


FIG. 4

- 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]. 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.

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."**

98. *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].

99. *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.

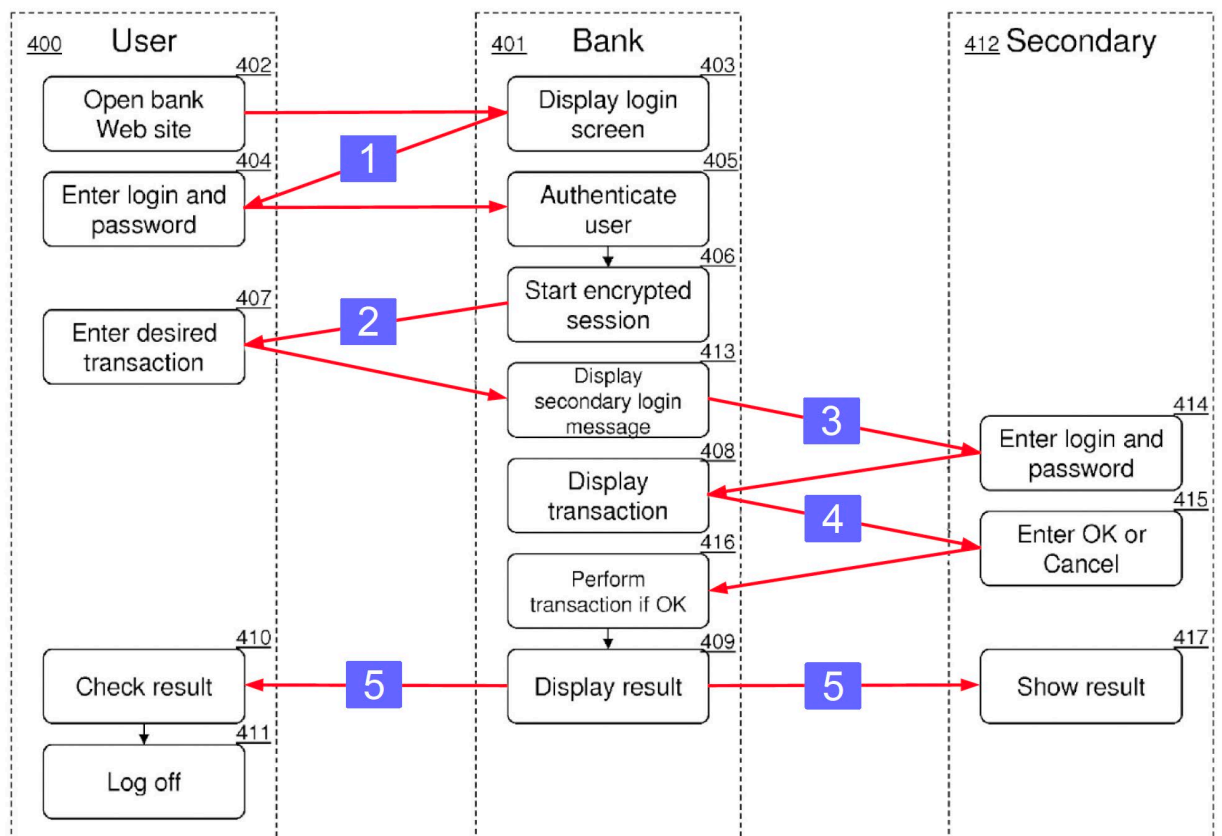
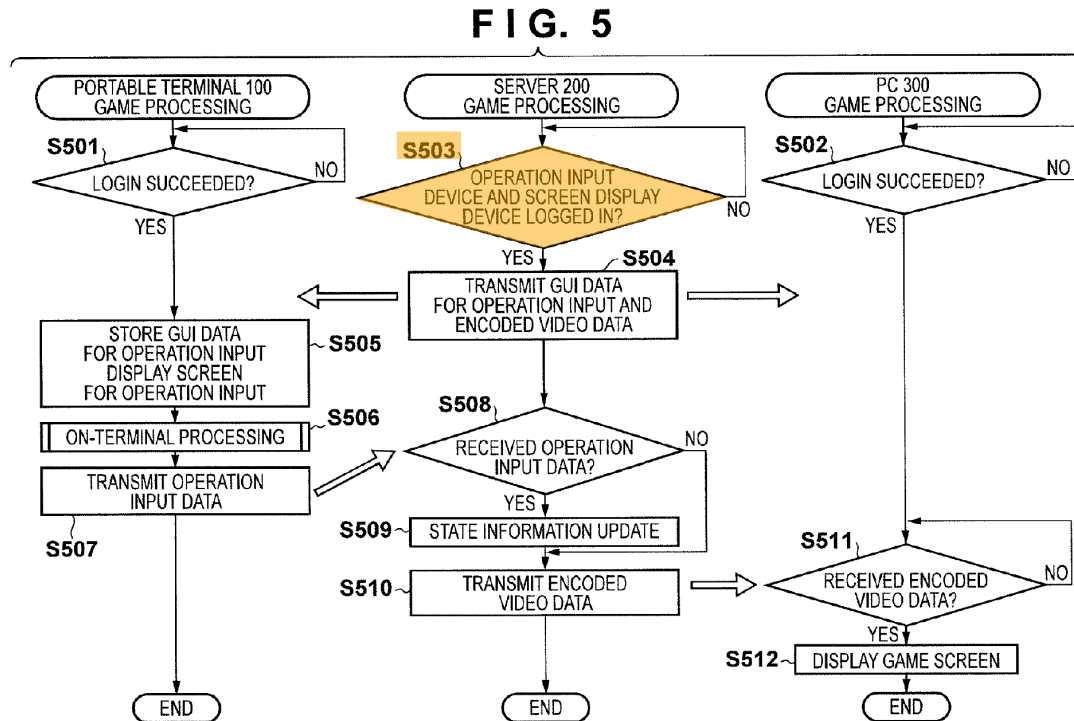


FIG. 4

- 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).

100. To the extent Patent Owner argues *Kling* does not disclose the “if and only if” limitation, 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 a server could be programmed to determine whether a user has successfully logged in via both the PC and the mobile device and refrain from transmitting data to either or both devices until both are logged in. For example, *Tsushima* (Ex. 1010) discloses “[i]n step S503, the server CPU 201 determines ***whether or not login to a service succeeded on both*** an operation input device (the portable terminal 100) and a screen display device (the PC 300) for a user ID that is a target of service provision.” Ex. 1010, [0059] (emphasis added). As shown in Figure 5, “when [the server] determines [at S503] that login has not succeeded for both devices, it repeats the processing of this step.” Ex. 1010, [0061].



Ex. 1010, Figure 5 (annotated).

101. “If and only if” both devices have successfully logged in (e.g., “YES” at step S503 in Figure 5), *Tsushima* expressly discloses transmitting different subsets of data to (1) the operation input device (the portable terminal 100) and (2) a screen display device (the PC 300): “In step S504, the server CPU 201, transmits GUI data for game content operation input from the server communication unit 206 to the portable terminal 100 registered as an operation input device . . . Also, in this step, the server CPU 201 initiates provision of encoded video data to the PC 300 registered as the screen display device.” Ex. 1010, [0062]-[0063].

102. *Tsushima* is evidence of a POSITA’s general knowledge at the time of the ’376 patent application, i.e., that a POSITA would know how to implement an

“if and only if” function such as *Tsushima*’s step S503. It is my opinion a POSITA would have used this function in *Kling*’s system because (1) *Kling* expressly discloses that its system is directed to a user using the PC and the mobile device simultaneously and (2) *Kling* sought to avoid unwanted malware by using two different passwords to separately login on two devices. Ex. 1023, Figure 5, [0019].

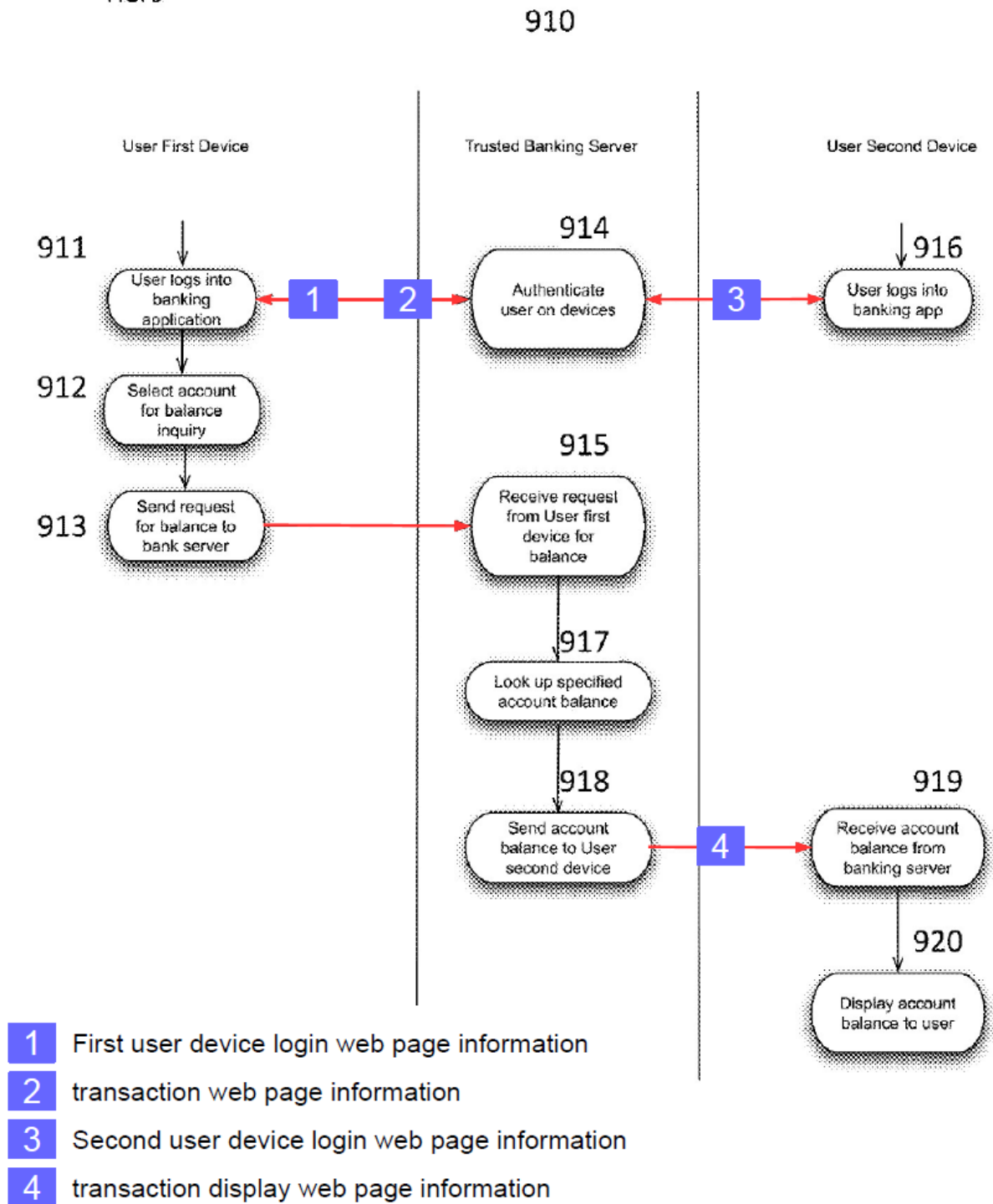
103. It is my opinion that *Kling*’s goal of preventing malware breaches in a banking application would motivate a POSITA to implement the “if and only if” function in *Kling* and it is also my opinion that a POSITA would be successful in modifying *Kling* to require both the PC and the mobile device to be logged in and accessible prior to sending the “display transaction” Web site page (408/508) because *Kling* does not send that pages until after the user has logged in to each device, respectively.

104. For the foregoing reasons, it is my opinion the subject matter of substitute claim 26 is rendered obvious by *Kling* alone or combined with the POSITA’s general knowledge (as demonstrated in *Tsushima*).

105. 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, Figure 9, 9:65-10:7.

FIG. 9



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

106. Similarly, *Kling* 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.

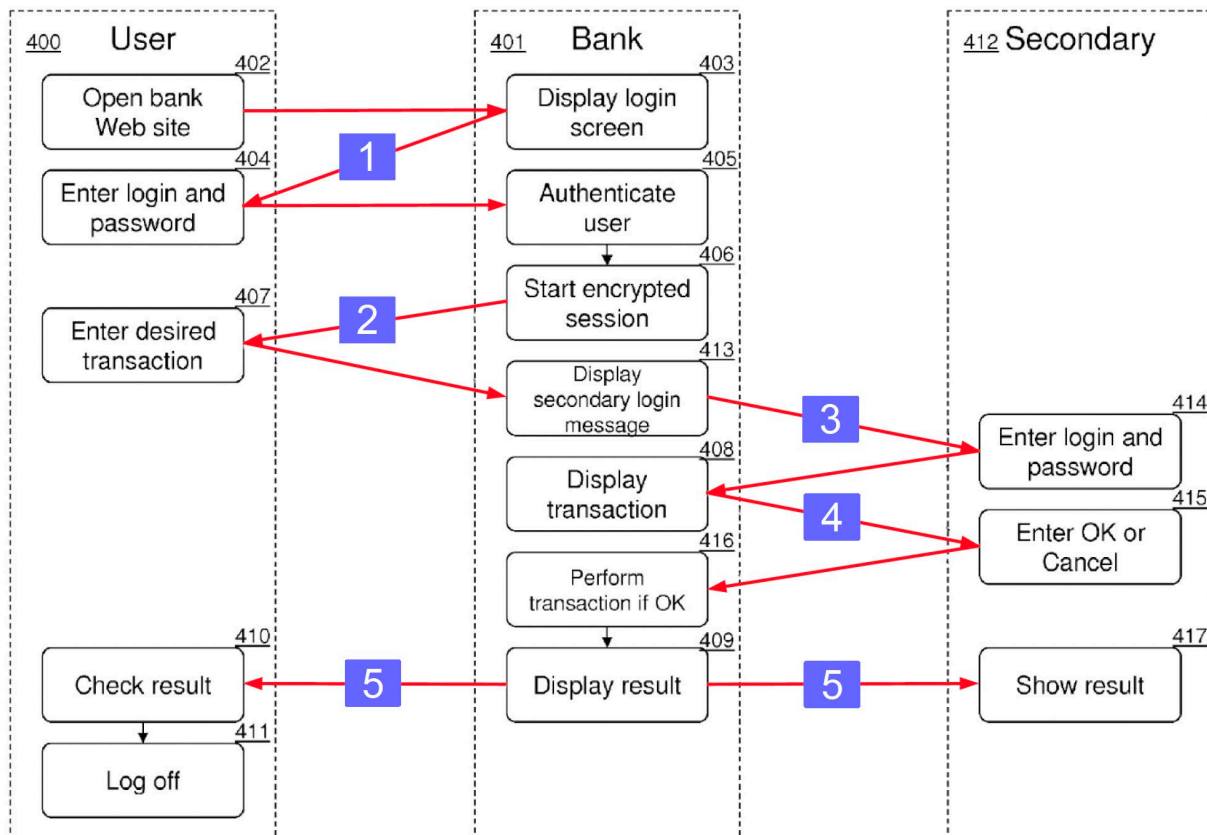


FIG. 4

- 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 page information

107. *Kling* discloses a nearly identical 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. *Compare* Ex. 1001, Figure 9 and 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, and 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. Thus, the *Kling* discloses the [26d] “if and only if” limitation.

C. Substitute Claim 27 — “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.”

108. *Kling* discloses this element. 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 claim 26.

109. *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 corresponds 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."

110. 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* renders this “only if” limitation obvious for the same reasons as discussed above for claim 26, namely, *Kling* discloses the “only if” condition and, if not, it would be obvious based on a POSITA’s general knowledge.

D. Substitute Claim 28 — “the first subset of the information comprises *non-sensitive information*; and the second subset of the information comprises sensitive information”

111. *Kling* discloses this element. *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. 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 (the “OK” response) is clearly sensitive.

112. *Kling* teaches the “desired transaction” is only 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 “desired transaction” from the malware, *Kling* clearly teaches the “desired transaction” is “sensitive information,” as claimed.

E. Substitute Claim 29 — “wherein the information received at the second device is more sensitive than the information received at the first device”

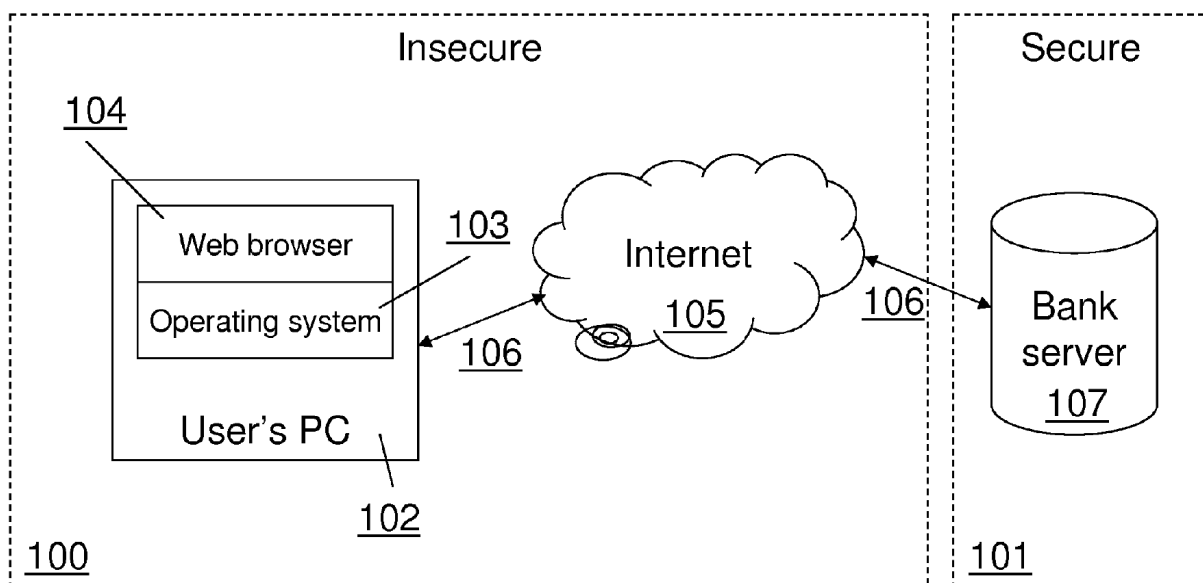
113. *Kling* discloses this element. *Kling* discloses the user may log into a banking application via both the user’s PC and the user’s mobile device. Ex. 1023, [0014] and [0017]. As noted above, the transaction web page information [Arrow #2] generated by the bank server 401 to “start encrypted session” 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.

114. *Kling* teaches the “desired transaction” 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 “desired transaction” 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.

F. Substitute Claim 31 — “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.”

115. *Kling* discloses this element. 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.

116. 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.

117. 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.

118. 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.

G. Substitute Claim 34 — “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”

119. *Kling* discloses this element. *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. Further, the transaction confirmation web page [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.

120. *Kling* shows a flow chart for sending subsets of information exclusively to the first user 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 PC login web page information [Arrow #1] so the user may “enter login and password” 404 on the PC. After 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 transaction web page information [Arrow #2] to the PC for exclusive viewing by 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 (phone login web page information [Arrow #3]) to the mobile device for the user to “enter login and password” 414. After the user is authenticated on the mobile device, then the remote bank server 401 generates and sends a “display transaction” 408 transaction confirmation web page information [Arrow #4] for exclusive

viewing by the user on the mobile device, and the user may “enter OK or cancel”
415 on the mobile device.

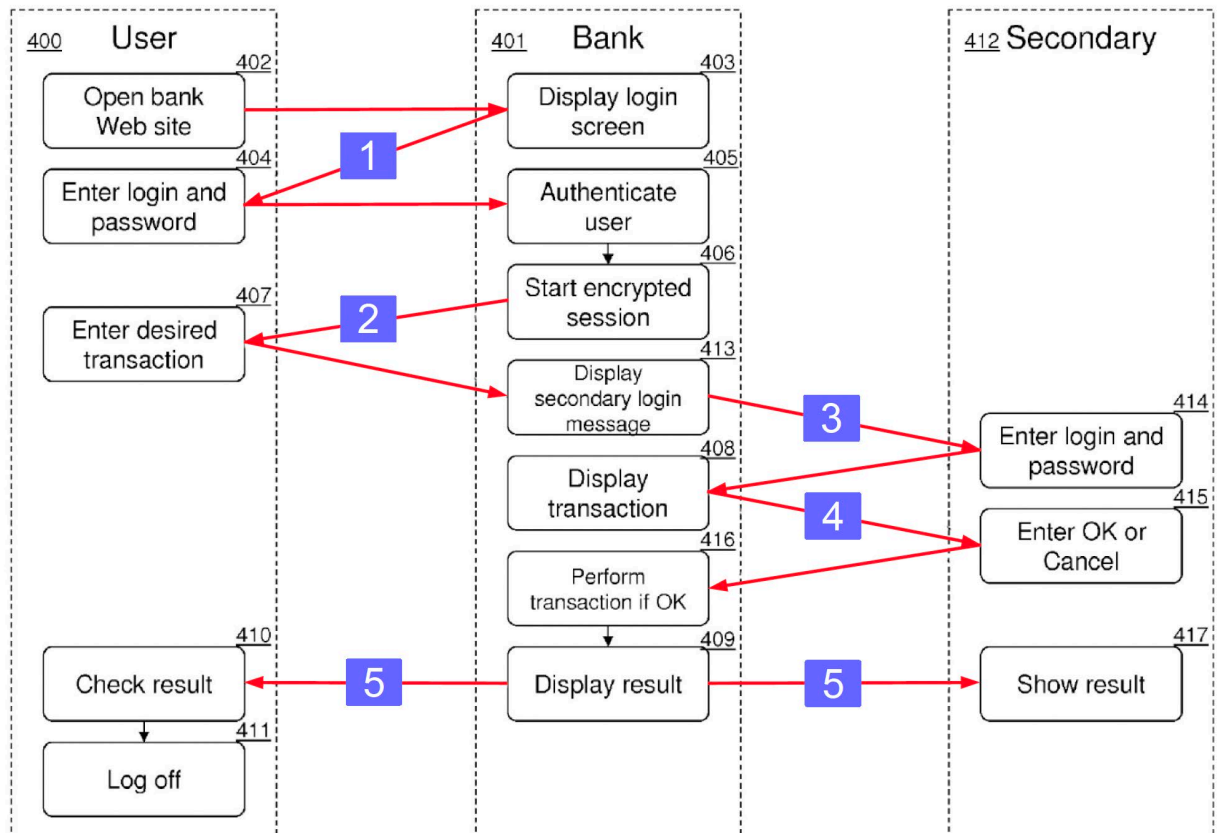


FIG. 4

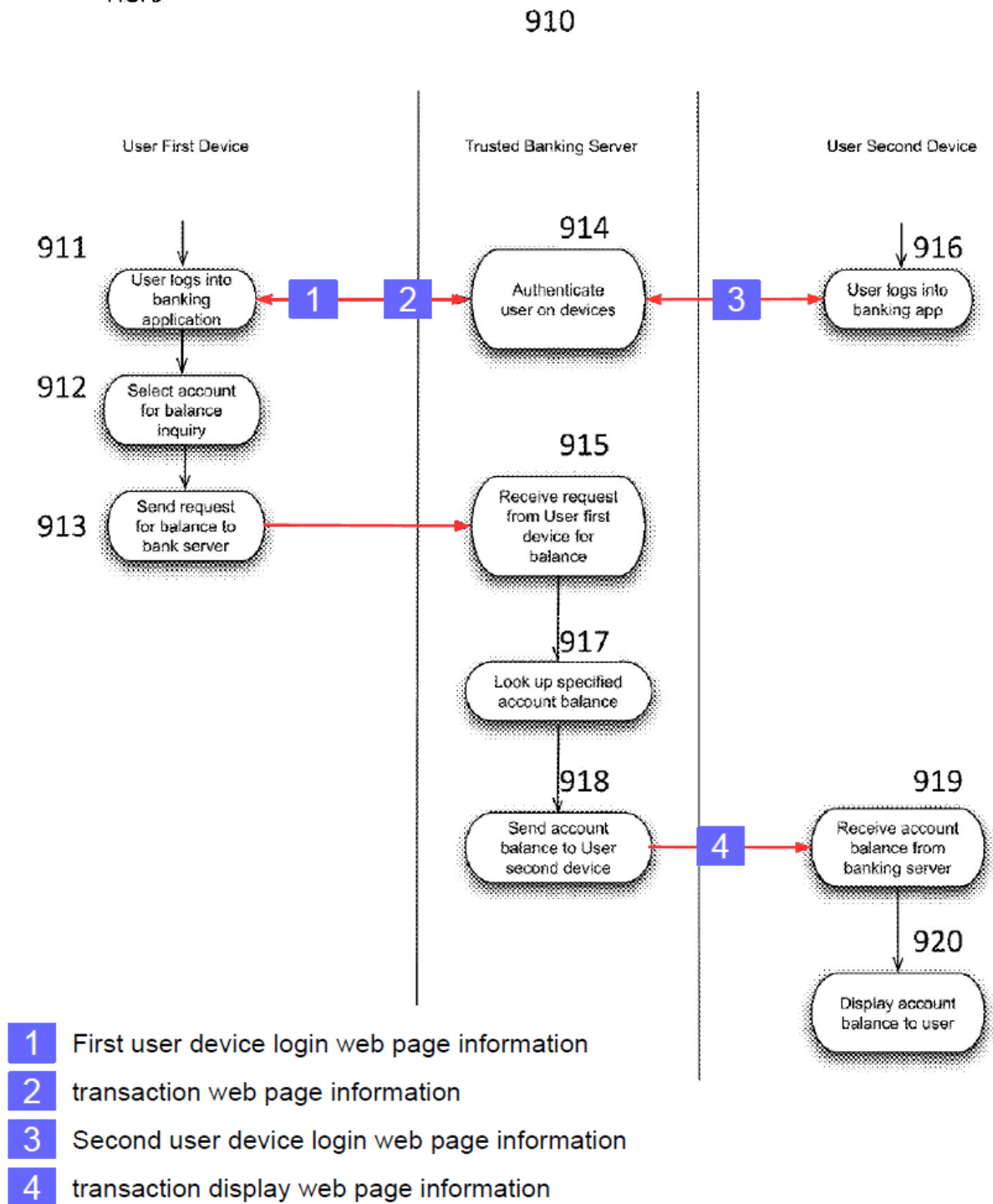
- 1 PC login web page information
- 2 transaction web page information
- 3 phone login web page information
- 4 transaction confirmation web page information
- 5 results page information

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

121. 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 claim 34’s “exclusive viewing” 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, Figure 9, 9:65-10:7.

FIG. 9



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

122. Similarly, *Kling* meets claim 34’s “exclusive viewing” limitation where the “bank server” 401 logs in the user on both a user PC and a user’s mobile device, using different passwords, and after the user is authenticated sends subsets of information.

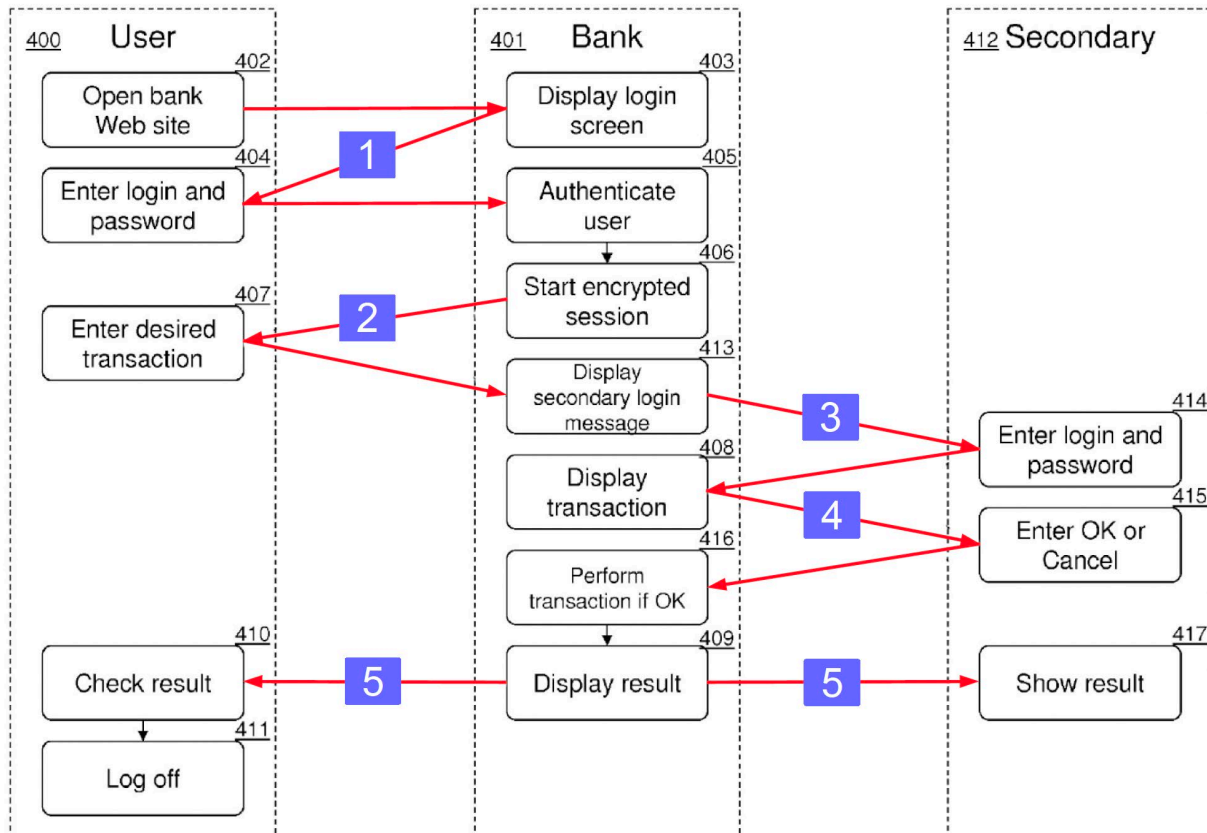


FIG. 4

- 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 page information

123. *Kling* discloses a nearly identical flow chart for sending subsets of information after the remote bank server 401 authenticates the user on the PC and

the mobile device. *Compare* Ex. 1001, Figure 9 and Ex. 1023, Fig. 4. The remote bank server 401 generates and sends a “display login screen” 403 (PC login web page information [Arrow #1]) so the user may “enter login and password” 404 on the PC. After the remote bank server 401 has authenticated the user 405 on the PC, the remote bank server 401 “starts encrypted session” 406, and generates and sends a transaction web page information [Arrow #2] 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 (phone login web page information [Arrow #3]) to the mobile device for the user to “enter login and password” 414. After the user is authenticated on the mobile device, then the remote bank server 401 generates and sends a “display transaction” 408 transaction confirmation web page information [Arrow #4] to the mobile device, and the user may “enter OK or cancel” 415 on the mobile device. Thus, the *Kling* discloses the [34] “exclusive viewing” limitation.

H. Substitute Claim 40 — “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.”

124. *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.

I. Independent Substitute Claim 41

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

125. To the extent the preamble is limiting, *Kling* discloses this element. *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].

126. 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.

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”**

127. *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.”

128. 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.

129. 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.

130. 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.

131. *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.

132. 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, Figure 2, [0014]; 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.”). 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].

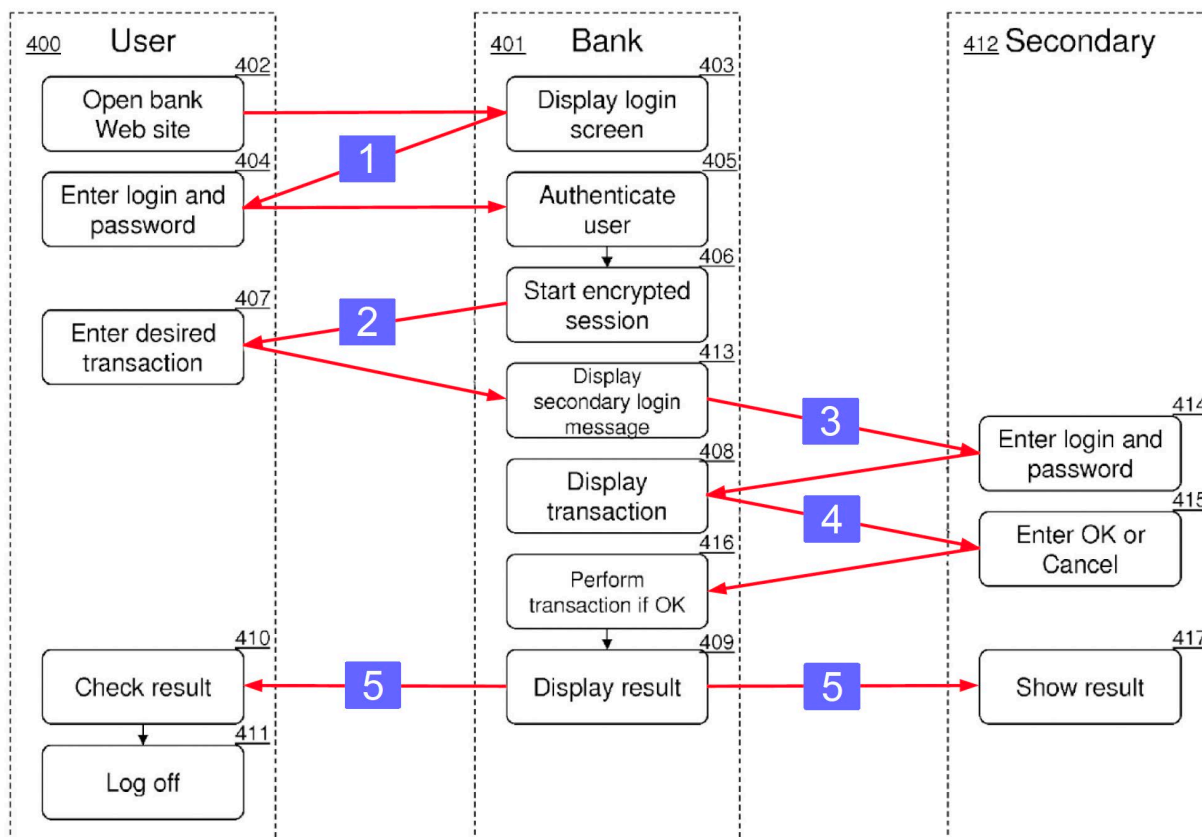


FIG. 4

- 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

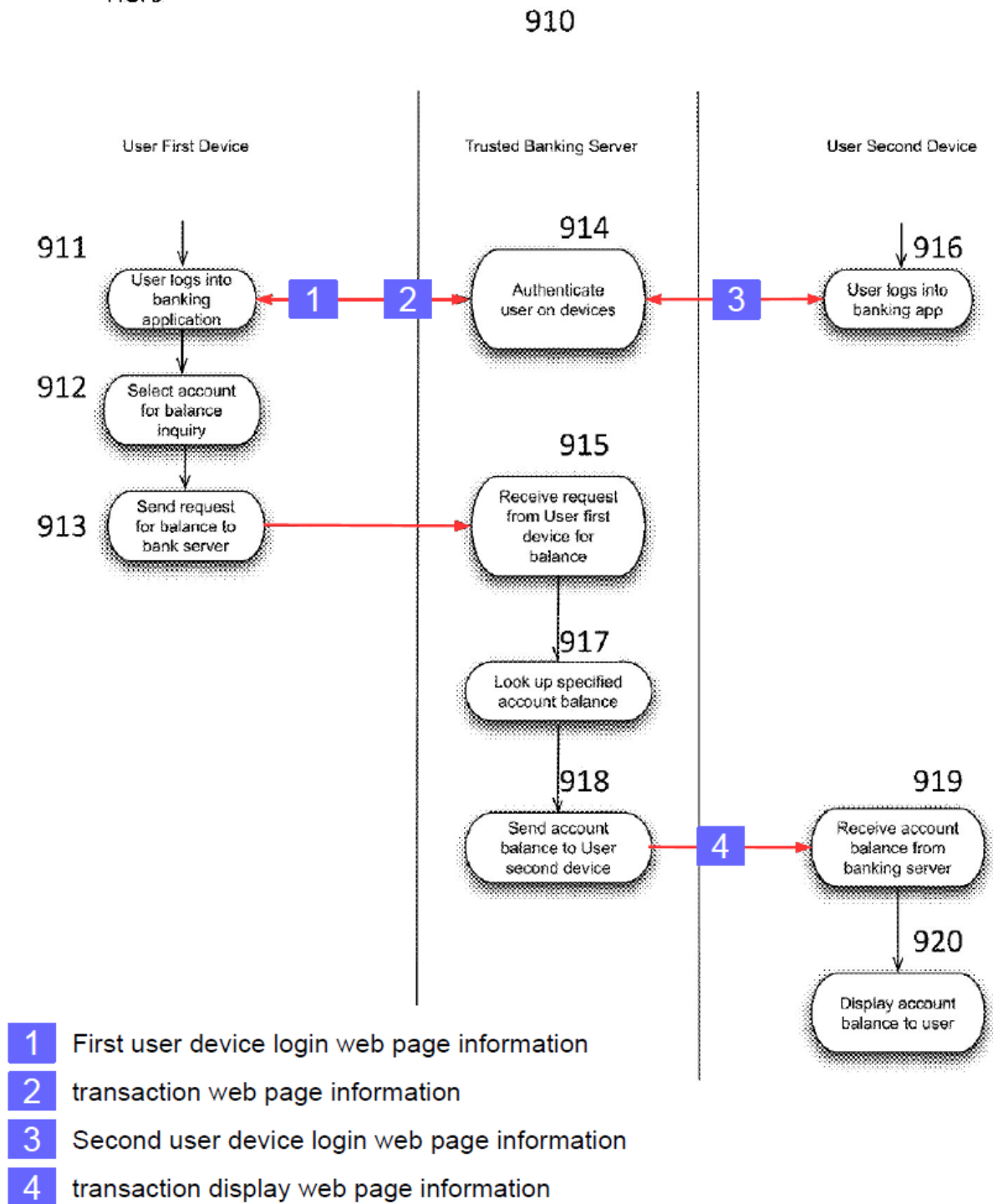
Ex. 1023, Figure 4 (revised and annotated).

133. 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.

134. *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.

135. 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.

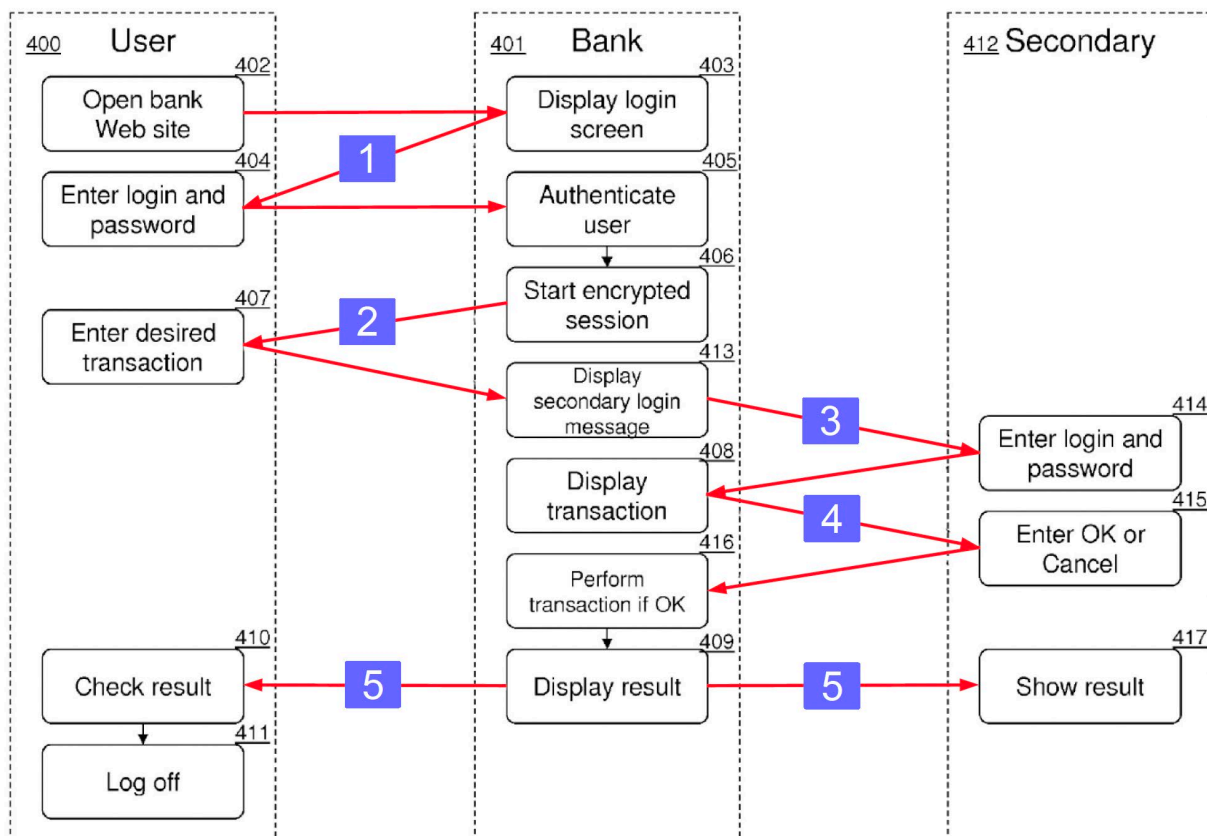


FIG. 4

- 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:”

136. *Kling* discloses this element. *Kling* discloses a remote Banking server 107, 201, 301, 401, and 501, 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;”

137. This element is also found in 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 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;”

138. This element is also found in substitute claim 26. *Kling* discloses this element as explained for 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.”

139. This element is also found in substitute claim 26. *Kling* discloses this element as explained for substitute claim element [26d].

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

A. Obviousness under 35 U.S.C. § 103

140. 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.

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

1. Substitute Claims 26 and 41

142. Substitute claims 26 and 41 are amended to add a new term “application specific authentication information” 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]).

143. Based on Patent Owner’s apparent understanding of the new limitations in 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 *Zha* and their own general knowledge.

144. Although I disagree that Patent Owner has identified sufficient written description support for the new term “application specific authentication information” (*see* discussion above), I evaluate the patentability of the substitute claims based on Patent Owner’s apparent reliance on the disclosure of using two different device 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,” using passwords with *Zha* would be obvious to a person of ordinary skill in the art.

145. 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 *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.

146. 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.

147. 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).

148. 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.

149. 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).

150. 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.

151. Here, both *Kling* and *Lipetz* are prior art patents that relate to the field of computer security, and more particularly, to securing computer systems against malware. *See* Ex. 1023, [0005] (“enhanced online transaction security”), [0015] (“the user’s local PC is compromised by Malware”); 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.”). Thus, both *Kling* and *Lipetz* 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, both *Kling* and *Lipetz* 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.

152. 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 *Kling*’s and *Lipetz*’s disclosure of

different passwords is high-level (and without much detail)—implementing a password authentication mechanism in an application was well within the POSITA's knowledge before 2014.

153. For the above reasons, it is my opinion a POSITA would use the POSITA's knowledge of multiple-password authentication schemes (as evidenced by *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 *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).

154. It is my opinion that this obvious modification of *Zha* to include multiple different passwords for the same user account renders 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. 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).

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

155. I understand that substitute dependent claims 27-29, 31-34, and 36-40 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 *Kling* for the same reasons discussed in Section IX.B (above).

3. Substitute Claim 30

156. I understand Patent Owner's amendment to substitute claim 30 (original claim 5) includes (1) depending from substitute claim 28 (original claim 3) instead of substitute claim 26 (original claim 1); and (2) adding the underlined limitation in "providing a notification by the application on the second device that

the connectivity has been disrupted.” I discuss above my opinion as to why this amendment lacks written description and why it is indefinite. Regardless, it is also my opinion that a POSITA would have found 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 *Kling*.

157. 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, *Kling* is evidence of the POSITA’s further knowledge of using multiple/different passwords to protect against malware when using different devices to access an online system. Section IX.B (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.

158. 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, as best understood. 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 by the application 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. Substitute Claim 35

159. 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 30, from which claim 35 depends, lacks written description and why it is indefinite. 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 *Kling*. Section IX.B (above).

160. 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)).

161. 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.

162. 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 *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 *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"

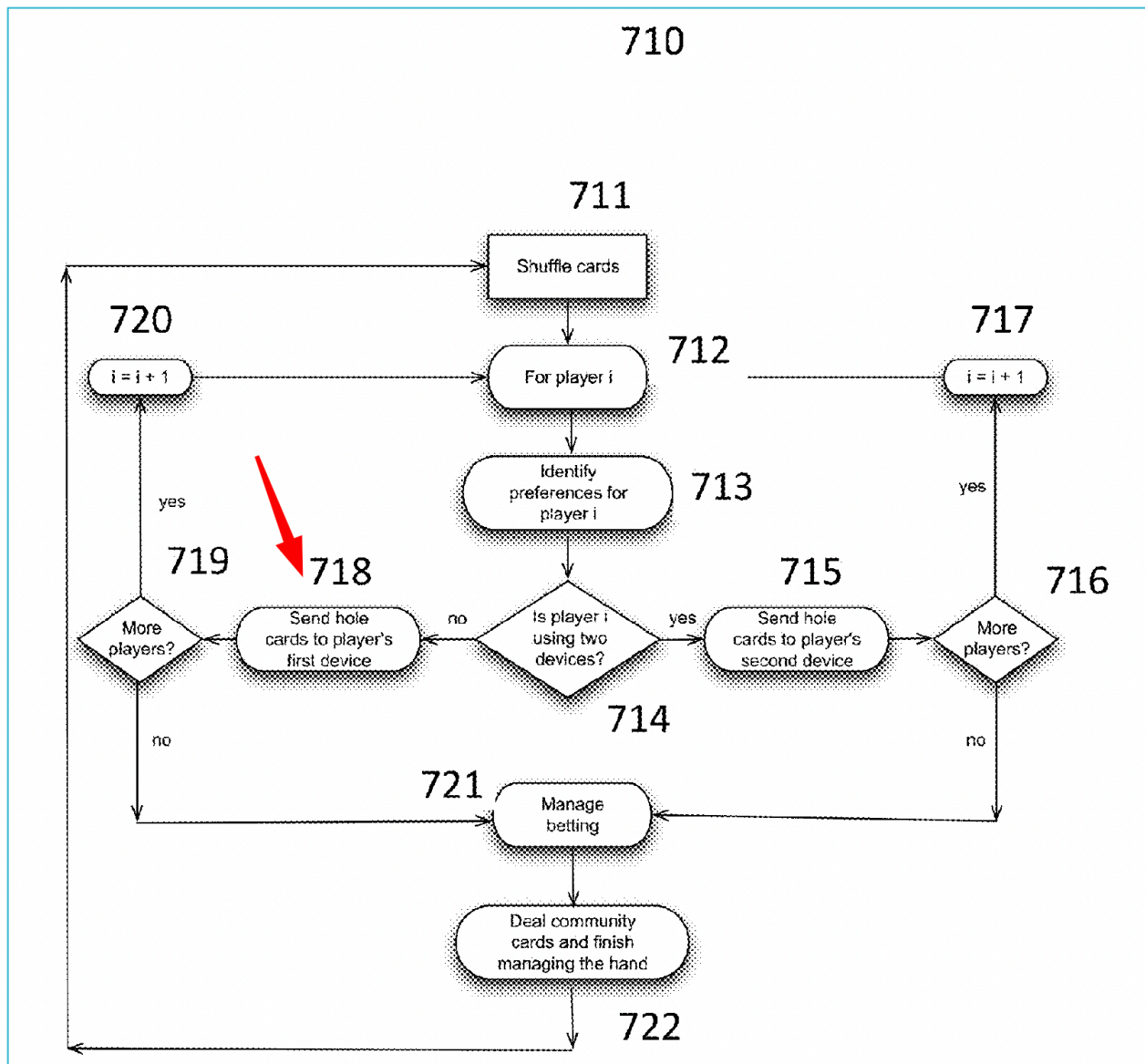
163. Patent Owner and its expert argue that "*Zha* does not mention or disclose the use of authentication information to determine if a first user is logged into the application. Motion to Amend ("MTA") at 13; Ex. 2004 ¶ 52. I disagree. *Zha* discloses that the "user may login to a microblog in the laptop 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 amended claims. Patent Owner's expert agrees with this conclusion. Ex. 1026, 71:9-17, 98:22-99:22. Thus, *Zha*'s disclosure of logging into the

microblog is a disclosure of using authentication information to determine if a first user is logged into the application.

2. “sensitive information”

164. Patent Owner and its expert argue that *Zha* does not disclose sending “sensitive information” to the second device. MTA at 14; Ex. 2004 ¶¶ 62-64. I disagree. First, I note these arguments rely, in part, on the Patent Owner’s claim construction of the term “sensitive information.” As explained above, I disagree with that claim construction and, for the same reasons, I disagree with Patent Owner’s arguments that rely on that claim construction.

165. Second, it is my opinion that *Zha*’s private message information would satisfy Patent Owner’s claim construction because *Zha* treats the private message information similarly to how the ’376 Patent treats sensitive information. 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 without first seeking the user’s permission. 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).

166. 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.

167. Because *Zha* works in substantially the same way as the '376 Patent, it is my opinion that *Zha*'s disclosure satisfies “sensitive information” even under Patent Owner's construction.

**3. “sensitive information” (i) generated by the application
(ii) at the server and (iii) specific to the application**

168. For substitute claims 28, 30, 35, 37, and 38, Patent Owner and its expert argue that *Zha* does not disclose “sensitive information” that is (i) generated by the application (ii) at the server and (iii) specific to the application. MTA at 14; Ex. 2004 ¶ 63. I disagree with this analysis.

169. First, Patent Owner's argument is based on a misreading of the claim language. Substitute claim 26 requires first “electronically storing a set of

information at a server” (element [26a]) and thereafter “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” (element [26b]). A POSITA would understand the subject of the “wherein” clause is “the first and second subsets of information” and that it is the *subsets* that “are generated by the same application at the server and are specific to that application.” In other words, the application is generating the subsets of information based on the complete information set. In contrast, Patent Owner and its expert incorrectly read the claim as requiring the *information* itself to be “generated by the same application at the server and [to be] specific to the application.” A POSITA would not understand the claim as Patent Owner and its expert have apparently construed it, especially in light of limitation [26a] which requires “electronically storing a set of information at a server.” This limitation does not put any qualifiers on the information itself—it can be any information from any source.

170. Second, Patent Owner’s argument that information must be generated by the application at the server conflicts with the embodiments disclosed in the ’376 Patent. Indeed, the ’376 Patent embodiments use pre-existing information that was not generated by the application itself at the server. For example, in the healthcare embodiment, the sensitive information is a user’s medical records. Ex. 2005-018, ¶

77. A POSITA understands that the medical records are created by doctors or other healthcare providers and are not “generated by the application” or “at the server” as Patent Owner argues. Similarly, Dr. Traynor testified during his deposition that a social security number would be “sensitive information.” Ex. 1026, 41:18-42:4. Social security numbers are not generated by an application “at the server” that uses them. Rather, social security numbers are generated by the government.

171. Third, Dr. Traynor argues that *Zha*’s private messages cannot be “sensitive information” because “private messages are not specific to any application . . . [and] users could send and/or exchange their private messages on any messaging application.” Ex. 2004 ¶ 63; *see also* MTA at 14. I note that the same argument could be made for each of the embodiments disclosed in the ’376 Patent. Users could play poker on any poker application, users could perform online banking tasks on any online banking application, and users could access healthcare records on any online healthcare application.

172. For at least these reasons, I disagree with Patent Owner’s and Dr. Traynor’s argument that *Zha*’s private messages are not “sensitive information” as that term is used in the substitute claims.

4. Motivation to combine *Zha* with POSITA’s knowledge, *Tsushima* and “analogous” art

173. Patent Owner argues *Zha* and *Tsushima* are not “analogous” prior art and there is no motivation to combine *Zha* with the general knowledge of a POSITA

or to combine *Zha* with *Tsushima* because these references are “extremely far afield from the field of endeavor for the ’376 Patent, and each seeks to address an unrelated problem,” and the ’376 Patent has “much broader application in the field of online security.” MTA at 19-25. I disagree.

174. First, I am advised that prior art references are to be considered for all they teach to a person of skill in the art. *Zha* and *Tsushima* each disclose systems that require the authentication of a user at multiple devices using login credentials. Ex. 1004, *Zha*, 9:20-38 (“the server can receive a login request sent by each terminal” and assign an access permission “to each terminal which has successfully logged in, after receiving the login request sent by each terminal”); Ex. 1010, *Tsushima*, [0057] (“In a case where the server CPU 201 determines that login has succeeded for both an operation input device and a screen display device for a provision target user ID, it moves the processing to step S504, and when it determines that login has not succeeded for both devices, it repeats the processing of this step.”). As evidenced by a 2006 article co-authored by Patent Owner’s expert, it was well known by 2014 that password authentication mechanisms were the dominant authentication mechanism used to authenticate a user logging into online computer systems such as *Zha* and *Tsushima*. Ex. 1024 at 37 (PDF page 1). Thus, each of these prior art references suggests to a person of skill in the art that they are

within the field of online security since they each expressly discloses systems and methods for addressing user authentication in online computer systems.

175. It is my opinion that for at least the reason just discussed, a POSITA would understand these prior art references to be related to the field of online security regardless whether the specification or claims in these prior art references use the exact terms “security” or “malware.” For instance, they teach security-related features such as privacy protection, access rights, and user authentication (e.g., via login mechanisms). *See* Ex. 1004, 6:58-59 (“the user may login”), 9:18-21 (“the terminal sends a login request to the server with an account first when applying for accessing the application program”), 9:23-25 (“the server may automatically assign an access permission for accessing at least one functional interface”), 13:32-33 (“the user only wants the private message interface to be displayed on the cellphone”); Ex. 1010, [0057] (“receives account information input from the user and determines whether or not login . . . succeeded”).

176. Second, Patent Owner’s substitute claims require “determining at the server whether both [first and second devices] 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.” *Zha* and *Tsushima* each disclose that a server determines whether a user has “logged” into multiple devices. Ex. 1004, *Zha*, 9:20-38; Ex. 1010,

Tsushima, [0057]. Thus, *Zha* and *Tsushima* specifically address the same problem addressed by the substitute claims.

177. Third, Patent Owner and its expert argue there is no motivation to combine *Zha* with the POSITA's knowledge or other prior art because "unless an application program has more than one functional interface to choose from, there is no reason to apply the teachings of *Zha* in order to reduce the network traffic or lower the amount of switching between functional interfaces to decrease 'operational complexities.'" MTA at 24; Ex. 2004 ¶ 61. I note that each of the prior art systems here, including *Zha*, *Tsushima*, *Takahashi*, *Kling*, and *Stafford*, all have separate functional interfaces on the separate terminals (e.g., laptop interface is different from the smartphone interface). The same is true of the '376 Patent, which includes different functional interfaces on the main display versus the phone display. Ex. 1001, Figures 6, 8. Accordingly, each of the prior systems provides the reason to apply the teachings of *Zha*, as Patent Owner and its expert have argued (i.e., they have more than one functional interface). The presence of two functional interfaces further confirms that *Zha* and the other prior art are solving a similar problem address by the substitute claims.

178. Fourth, Patent Owner and its expert argue that a POSITA would not combine *Zha* and *Tsushima* to arrive at the claims of the '376 Patent because the claims are allegedly "device agnostic" whereas *Tsushima* is "device specific," which

appears to mean that *Tsushima* requires a PC and a portable terminal. MTA at 24; Ex. 2004 ¶ 80. I note that a POSITA reading *Tsushima* would understand *Tsushima* to be providing examples of the different terminals that “may” be used (Ex. 1010 ¶ 28), and thus would not understand *Tsushima* to be as limited as Patent Owner claims. But even if Patent Owner and its expert were correct in their characterization of *Tsushima*, that would not change my opinion that *Zha* and *Tsushima* are properly combined to arrive at the substitute claims. In particular, *Tsushima* is relied upon to show a POSITA would know about the claimed “if and only if” functionality, i.e., that information could be sent to two separate devices, regardless of what specific types of devices they are, “if and only if” it is determined that the two devices are logged in (and satisfy the other requirements of the claim). In other words, the functionality in *Tsushima* used in the combination is itself device agnostic (according to Patent Owner’s characterization).

179. For at least these reasons, it is my opinion a POSITA would have been motivated to combine *Zha* with the general knowledge of a POSITA or to combine *Zha* with *Tsushima* because each of these prior art references are within the field of online security and address the specific problem of authenticating a user via login on two devices each having different functional interfaces.

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

180. 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).

181. It is my opinion a POSITA would be motivated to combine *Kling* with the other prior art (Grounds 1-6) for the same reasons I provide above in Section X.B.4, 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 *Kling*'s disclosure of using multiple/different passwords to protect against malware in systems accessing sensitive (and less- or non-sensitive) information with different devices.

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

A. Obviousness under 35 U.S.C. § 103

182. 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.

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

1. Substitute Claims 26 and 41

184. Substitute claims 26 and 41 are amended to add a new term “application specific authentication information” 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]).

185. I first note that *Takahashi* discloses “identification information” that is used by the application along with the password and user ID during the authentication process. Ex. 1007, [0110]. *Takahashi* discloses that this identification information is “unique information for each mobile terminal.” Ex. 1007, [0074]. Patent Owner does not dispute this. *See* MTA at 17; Ex. 2004 ¶ 93. Patent Owner and its expert instead argue that *Takahashi*’s identification information is “device specific” and, thus, not “application specific.” I disagree. *Takahashi* discloses that the identification information is used by the application to authenticate the user when the user logs in with a main terminal and sub-terminal. Ex. 1007, [0073]-[0080], [0110]. The “identification information is recorded in association with user ID for the purpose of the subsequent user authentication.” Ex. 1007, [0075]. Further, “the identification information is incorporated into the user agent character string in the

HTTP request upon the user's permission.” *Id.* Based on these passages, a POSITA would understand that the identification information is used by the application in the current and subsequent user accesses. Accordingly, a POSITA understands this identification information to be “application specific” and different (unique) for each of the user's terminals. For this reason, it is my opinion that *Takahashi* expressly discloses the new limitations of substitute claims 26 and 41.

186. Alternatively, based on Patent Owner's apparent understanding of the new limitations in 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.

187. Although I disagree that Patent Owner has identified sufficient written description support for the new term “application specific authentication information” (*see* discussion above), I evaluate the patentability of the substitute claims based on Patent Owner's apparent reliance on the disclosure of using two different device specific 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).

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

189. 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 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.

190. 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.

191. U.S. Patent No. 7,865,950 (“*Lipetz*”), which was filed in 2007 and issued in 2011, 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).

192. 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.

193. 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., *Takahashi*’s game system that includes sensitive, user-specific information (Ex. 1002 ¶ 318 (citing “game results for respective users, or items and objects, etc., which the user owns in the game” (Ex. 1007, [0120])))). 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 *Takahashi*’s more sensitive information (e.g., user-specific game results, etc.).

194. 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 of suggestion in the references themselves.

195. Here, both *Kling* and *Lipetz* are prior art patents that relate to the field of computer security, and more particularly, to securing computer systems against malware. *See* Ex. 1023, [0005] (“enhanced online transaction security”), [0015] (“the user’s local PC is compromised by Malware”); 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.”). Thus, both *Kling* and *Lipetz* 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, both *Kling* and *Lipetz* provide a motivation to combine a POSITA’s knowledge of using different passwords with *Takahashi*’s game application—i.e., to enhance security against malware in *Takahashi*’s computing system.

196. 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, *Kling*’s and *Lipetz*’s disclosure of different passwords 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.

197. For the above reasons, it is my opinion a POSITA would use the POSITA’s knowledge of multiple-password authentication schemes (as evidenced

by *Kling*) 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 *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).

198. It is my opinion that this obvious modification of *Takahashi* to include multiple different passwords for the same user account renders 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. Substitute Claims 27-29, 31-34, and 37-41

199. 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 *Kling* for the same reasons discussed in Section XII.B.4 (above).

3. Substitute Claim 30

200. I understand Patent Owner's amendment to substitute claim 30 (original claim 5) includes (1) depending from substitute claim 28 (original claim 3) instead of substitute claim 26 (original claim 1); and (2) adding the underlined limitation in "providing a notification by the application on the second device that the connectivity has been disrupted." I discuss above my opinion as to why this

amendment lacks written description and why it is indefinite. Regardless, it is also my opinion that a POSITA would have found 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 *Kling*.

201. In particular, I previously explained why *Takahashi* and a POSITA's general knowledge rendered original claim 5 obvious (Ground 7) and, alternatively, why *Zha*, a POSITA's general knowledge, and *Tsushima* rendered original claim 5 obvious (Ground 8). As discussed above, *Kling* is evidence of the POSITA's further knowledge of using multiple/different passwords to protect 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.

202. It is my opinion that *Takahashi* similarly discloses Patent Owner's new 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. Substitute Claim 35

203. 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 30, from which claim 35 depends, lacks written description and why it is indefinite. 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 *Kling*.

204. 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).

205. 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.

206. 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 *Kling*) or, alternatively, by *Zha*, a POSITA's general knowledge, and *Tsushima* (Ground 8 and the POSITA's general knowledge of multiple/different passwords as disclosed in *Kling*).

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

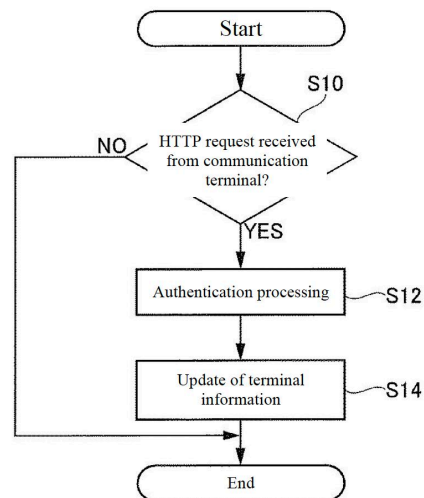
1. Login process followed by an authentication process

207. 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. MTA at 16-17; Ex. 2004 ¶¶ 91-92. I disagree.

208. 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

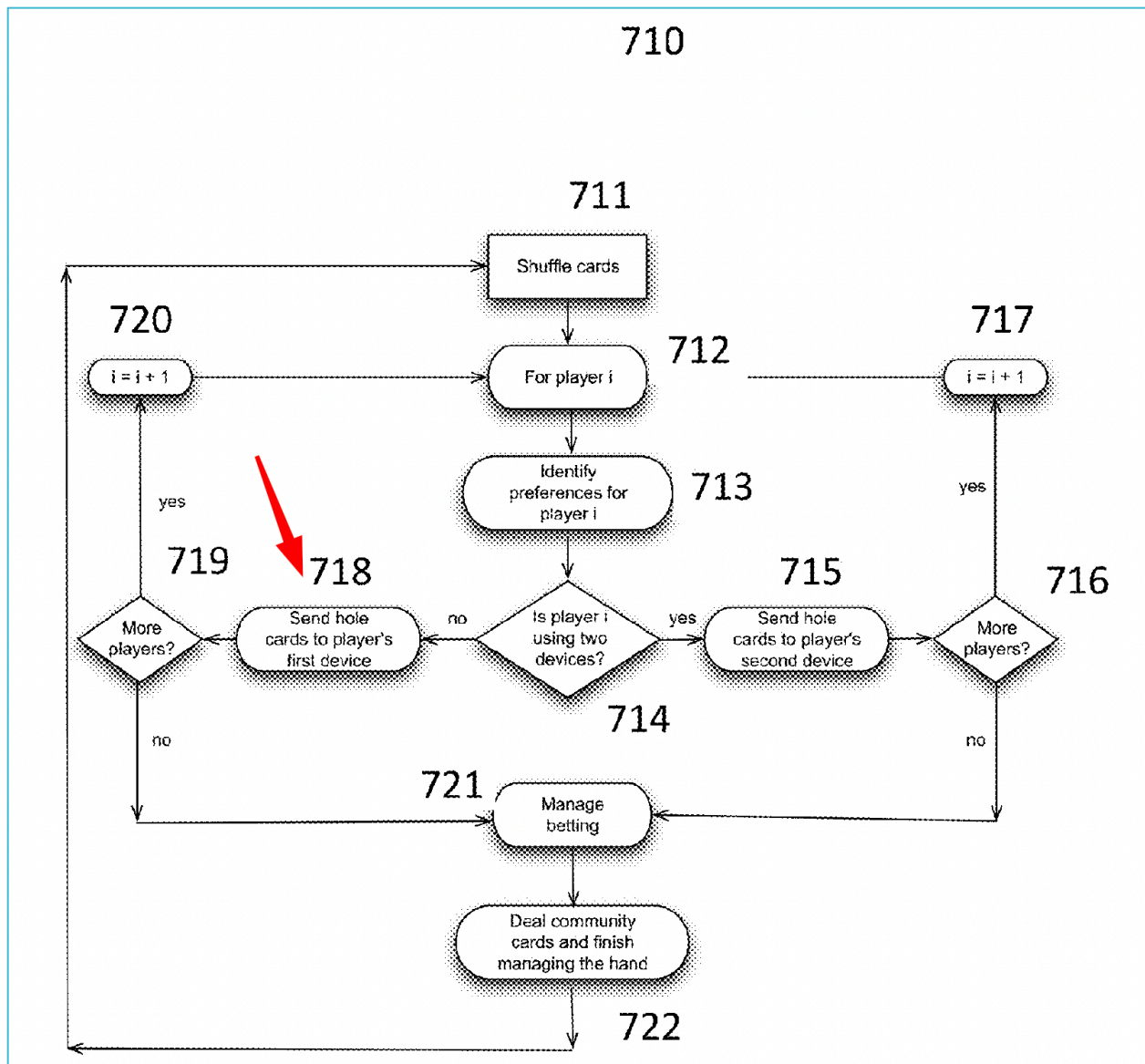
Ex. 1009-57 (red arrow added).

2. “sensitive information”

209. For substitute claims 28, 30, 35, 37, and 38, Patent Owner and its expert argue that *Takahashi* does not disclose “sensitive information.” MTA at 18-19; Ex. 2004 ¶¶ 101-105. I disagree. First, I note these arguments rely, in part, on the Patent Owner’s claim construction of the term “sensitive information.” As explained above,

I disagree with that claim construction and, for the same reasons, I disagree with Patent Owner's arguments that rely on that claim construction. E.g., Ex. 2004 ¶ 103.

210. Second, it is my opinion that *Takahashi*'s game results (one example of the "sensitive information" in *Takahashi*) would satisfy Patent Owner's claim construction because *Takahashi* treats the private message information similarly to how the '376 Patent treats sensitive information. A POSITA understands that if a user of *Takahashi*'s game has only one device the game results will be sent to that device. Dr. Traynor agrees. Ex. 2004 ¶ 103 ("*Takahashi*'s 'game results' are shared with the user's first device if/when the user plays their fishing game on a single 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 without first seeking the user's permission. 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).

211. Similarly, a POSITA understands that a user can use a second device (e.g., a mobile device) with *Takahashi's* game application so that the user-specific information (user's score or game results) is sent to the mobile device and not the main terminal. Ex. 1007, [0120]. In this scenario, a POSITA understands that *Takahashi* will not send that information to the main terminal. A POSITA understands that the '376 Patent discloses the same type of arrangement where the

user-specific information is not sent to the first device when “the user can be forced to sit out until such time as the user’s two devices are reachable.”

[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 to -009.

212. Because *Takahashi* works in substantially the same way as the ’376 Patent, it is my opinion that *Takahashi*’s disclosure satisfies “sensitive information” even under Patent Owner’s construction.

213. Finally, I note that neither Patent Owner nor its expert dispute my conclusion in my first declaration that even if it is argued that *Takahashi* does not expressly disclose “sensitive information” and “non-sensitive information” (claim 3, now substitute claim 28) or “more sensitive” information (claim 4, now substitute claim 29), it is my opinion that these limitations would have been obvious based on *Takahashi* and a POSITA’s general knowledge of other games that could be played using *Takahashi*’s system. Ex. 1002 ¶¶ 318-330. The other games include poker, which includes hole cards that are “sensitive information” under any definition of that term.

3. Motivation to combine *Takahashi* with POSITA's knowledge, *Tsushima*; Prior art is “analogous”

214. Patent Owner argues *Takahashi* and *Tsushima* are not “analogous” prior art and there is no motivation to combine *Takahashi* with the general knowledge of a POSITA or to combine *Takahashi* with *Tsushima* because these references are “extremely far afield from the field of endeavor for the '376 Patent, and each seeks to address an unrelated problem,” and the '376 Patent has “much broader application in the field of online security.” MTA at 19-25.

215. First, I am advised that prior art references are to be considered for all they teach to a person of skill in the art. *Takahashi* and *Tsushima* each disclose each disclose systems that require the authentication of a user at multiple devices using login credentials. Ex. 1009, *Takahashi*, [0110]-[0111] (“In the authentication processing, the identification information, or the user ID and the password, which are included in the HTTP request, are identified first” and “the game server 20 identifies a main-terminal and a sub-terminal of the user whose access request has been accepted.”); Ex. 1010, *Tsushima*, [0057] (“In a case where the server CPU 201 determines that login has succeeded for both an operation input device and a screen display device for a provision target user ID, it moves the processing to step S504, and when it determines that login has not succeeded for both devices, it repeats the processing of this step.”). As evidenced by a 2006 article co-authored by Patent Owner's expert, it was well known by 2014 that password authentication

mechanisms were the dominant authentication mechanism used to authenticate a user logging into online computer systems such as *Zha* and *Tsushima*. Ex. 1024 at 37 (PDF page 1). Thus, each of these prior art references suggests to a person of skill in the art that they are within the field of online security since they each expressly discloses systems and methods for addressing user authentication in online computer systems.

216. It is my opinion that for at least the reason just discussed, a POSITA would understand these prior art references to be related to the field of online security regardless whether the specification or claims in these prior art references use the exact terms “security” or “malware.”

217. Second, Patent Owner’s substitute claims require “determining at the server whether both [first and second devices] 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.” *Takahashi* and *Tsushima* each disclose that a server determines whether a user has “logged” into multiple devices. Ex. 1009, *Takahashi*, [0110]-[0111]; Ex. 1010, *Tsushima*, [0057]. Thus, *Takahashi* and *Tsushima* specifically address the same problem addressed by the substitute claims.

218. Third, I disagree with Patent Owner’s suggestion that a POSITA would not look to *Takahashi* alone or in combination with other prior art because the ’376

Patent “relies exclusively on two devices” whereas *Takahashi* can be used with one device. MTA at 24-25; Ex. 2004 ¶ 100. I disagree the ’376 Patent “relies exclusively on two devices” because it teaches, “[a]t 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. 1001, 5:4-6. Further, a POSITA would read *Takahashi* for all that it discloses, including the two-device arrangement. This arrangement is directly relevant to the ’376 Patent claims and, thus, would be considered by a POSITA.

219. For at least the above reasons, it is my opinion that a POSITA would have been motivated to combine *Takahashi* with the general knowledge of a POSITA or to combine *Takahashi* with *Tsushima* because each of these prior art references are within the field of online security and address the problem of authenticating a user via login on two devices.

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

220. 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).

221. It is my opinion a POSITA would be motivated to combine *Kling* with the other prior art (Grounds 7-8) for the same reasons I provide above in Section

XII.B3, 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 *Kling*'s disclosure of using multiple/different passwords to protect against malware in systems accessing sensitive (and less- or non-sensitive) information with different devices.

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*”)