

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KAHOOT! ASA and KAHOOT! EDU, Inc., Petitioner,
v.

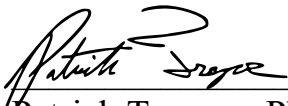
AVIEL D. RUBIN, Patent Owner.

Case IPR2023-00693
Patent 9,064,376 B1

**THIRD DECLARATION OF PATRICK
TRAYNOR, Ph.D.**

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 or Title 18 of the United State Code, and that such willful false statements may jeopardize the validity of the '376 Patent.

Date: June 14, 2024



Patrick Traynor, Ph.D

I. INTRODUCTION

1. My name is Patrick Traynor, Ph.D. I have been retained by Dr. Aviel D. Rubin which I may refer to as either the “Patent Owner” or “Dr. Rubin” for this *inter partes* review proceeding, which I may refer to as an “IPR.” I understand that this IPR proceeding involves U.S. Patent No. 9,064,376 (the “’376 Patent”). This declaration sets forth my opinions in response to (i) Petitioner’s Opposition to Patent Owner’s Revised Motion to Amend (the “Petitioner’s Opposition” or “Pet. Opp.”).

2. I will refer to Kahoot! ASA and Kahoot EDU, Inc. as collectively the “Petitioner” or “Kahoot” and I will refer to the Patent Trial and Appeal Board as the “Board.” I will refer to the Board’s March 20, 2024 Preliminary Guidance as “PG.”

3. I have reviewed and am familiar with the specifications, claims, and prosecution history of the ’376 Patent. Generally, I will cite to the ’376 Patent two ways. First, original Application 14/444,995 that gave rise to ’376 Patent is Patent Owner’s Exhibit 2003, and will be cited to as (Exhibit, Paragraph Number (s)). For example, the citation to paragraph seven of Application 14/444,995, will be Ex. 2003, ¶7. Second, I will cite to the specification of the ’376 Patent which is Petitioner’s Exhibit 1001, using column and line numbers (Exhibit, Column:

Line Number(s)). For example, the citation to the '376 Patent at column 1, lines 1 through 10, will be Ex. 1001, Col.1:1-10.

4. I have been asked to provide my objective, independent analysis of: (i) the Petitioner's Opposition, (ii) the asserted prior art references cited therein, and (iii) the supporting opinions of Dr. Sigurd Meldal (Ex. 1029).

5. I am not currently, nor have I ever been, an employee of Dr. Rubin. I received no compensation for this declaration beyond my normal hourly compensation of \$600/hr based on my time actually spent analyzing the '376 Patent, the Petitioner's Opposition, the asserted prior art references cited herein and in the Petition, and any related issues. I will not receive any added compensation based on the outcome of this IPR, Patent Owner's Revised Motion to Amend, any other IPR, or any other proceeding involving the '376 patent.

6. In forming my opinions expressed in this declaration, I have reviewed and, in some cases, relied upon the documents and other materials cited in Section III below, "Basis of Opinions and Materials Considered" in preparation of this declaration. To the best of my knowledge, those exhibits are true and accurate copies of what they purport to be. An expert in the field would reasonably rely on them to formulate opinions such as those set forth in this report.

7. This declaration contains opinions I formed with respect to the subject matter of this proceeding based on information available to date. I specifically

reserve the right to formulate and offer additional opinions based on any additional information or discovery that may be provided or derived, and I likewise reserve the right to supplement my opinions based on future discovery or disclosures, agreements between the parties, and additional evidence submitted by either party either prior to or at trial. I further reserve the right to supplement my opinions based on any expert testimony offered by Petitioner.

II. QUALIFICATIONS

8. My qualifications are listed in my Curriculum Vitae, which includes a complete list of my publications. Below, I summarize my qualifications and experience that qualify me to offer the opinions in this report as an expert.

9. I earned a B.S. in Computer Science from the University of Richmond in 2002 and an M.S. and Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2004 and 2008, respectively. My dissertation, entitled "Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks," focused on security problems that arise in cellular infrastructure when gateways to the broader Internet were created.

10. I am currently a Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. I was hired under the "Rise to Preeminence" Hiring Campaign and serve as the Associate

Chair for Research in my Department. I also hold the endowed position of the John and Mary Lou Dasburg Preeminent Chair in Engineering.

11. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from 2008 to March 2014 at the Georgia Institute of Technology. I have supervised many Ph.D., M.S., and undergraduate students during the course of my career.

12. My area of expertise is security, especially as it applies to mobile systems and networks, including cellular networks. As such, I regularly teach students taking my courses and participating in my research group to program and evaluate software and architectures for mobile and cellular systems. I have taught courses on the topics of network and systems security, cellular networks, and mobile systems at both Georgia Tech and the University of Florida. I also advised and instructed the Information Assurance Officer Training Program for the United States Army Signal Corps in the Spring of 2010.

13. I have received numerous awards for research and teaching, including being named a Kavli Fellow (2017), a Fellow of the Center for Financial Inclusion (2016), and a Research Fellow of the Alfred P. Sloan Foundation (2014). I also won the Lockheed Inspirational Young Faculty Award (2012), was awarded a National Science Foundation (NSF) CAREER Award (2010), and received the Center for

Enhancement of Teaching and Learning at Georgia Tech's "Thanks for Being a Great Teacher" Award (2009, 2012, 2013).

14. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results are highly cited, and I have received multiple "Best Paper" Awards. I have also written a book entitled "Security for Telecommunications Networks", which is used in wireless and cellular security courses at a number of top universities.

15. I am a Senior Member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). I am also a member of the USENIX Advanced Computing Systems Association.

16. I serve as an Associate Editor for IEEE Security and Privacy Magazine, have been the Program Chair for eight conferences and workshops, and have served as a member of the Program Committee for over 50 different conferences and workshops. I am also currently the Security Subcommittee Chair for the ACM US Technology Policy Committee (USACM).

17. I was a co-Founder and Research Fellow for a private start-up, Pindrop Security, from 2012 to 2014. Pindrop provides anti-fraud and authentication solutions for Caller-ID spoofing attacks in enterprise call centers by creating and matching acoustic fingerprints. Pindrop Security currently employs over 200 people, and their technology is based off of my research (US Patent 9,037,113 B2).

18. I was a co-Founder and Chief Executive of a private start-up, CryptoDrop. CryptoDrop developed a ransomware detection and recovery tool to provide state of the art protection to home, small business, and enterprise users. This technology was also based off of my research (US Patent 10,685,114 B2).

19. I was also a co-Founder and Chief Executive of a private start-up, Skim Reaper. Skim Reaper developed tools to detect credit card skimming devices, and worked with a range of banks, international law enforcement, regulators, and retailers. This technology was also based off of my research (US Patent 10,496,914 B2).

20. I am a named inventor on ten US patents. These patents detail methods for determining the origin and path taken by phone calls as they traverse various networks, cryptographically authenticating phone calls, providing a secure means of indoor localization using mobile/wireless devices, detecting credit card skimmers, identifying cloned credit cards, and blocking ransomware from encrypting data. My curriculum vitae, attached as Appendix A, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

21. I am very familiar with and have substantial expertise in the area of information security, mobile systems, and networking.

III. MATERIALS CONSIDERED

22. I have reviewed the '376 Patent, including the challenged claims, and its prosecution history. I have also reviewed the Petition for inter partes review filed by Petitioner, Dr. Rubin's Motion to Amend and Revised Motion to Amend, the Petitioner's Opposition, the Board's Preliminary Guidance, as well as documents referenced in each of the above along with any attached Exhibits, including:

- 23. Ex. 1002: Declaration of Sigurd Meldal
- 24. Ex. 1004: U.S. Patent No. 9,497,565 ("*Zha*")
- 25. Ex. 1005: CN 2013/10674692 ("*Zha* Priority Application")
- 26. Ex. 1006: Certified English translation of the *Zha* Priority Application
- 27. Ex. 1007: U.S. Patent Pub. No. 2015/0011318 ("*Takahashi*")
- 28. Ex. 1008: PCT/JP2012/007595 ("*Takahashi* Priority Application")
- 29. Ex. 1009: Certified English translation of *Takahashi* Priority

Application

- 30. Ex. 1010: U.S. Patent Pub. No. 2014/0006485 ("*Tsushima*")
- 31. Ex. 1011: U.S. Patent No. 9,591,083 ("*Gumbula*")
- 32. Ex. 1012: U.S. Patent Pub. No. 2012/0017236 ("*Stafford*")
- 33. Ex. 1013: U.S. Patent No. 9,330,531 ("*Wakeford*")

34. Ex. 1014: 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)

35. Ex. 1015: U.S. Patent Pub. No. 2012/0253841 ("*'841 Application*")

36. Ex. 1016: U.S. Patent Pub. No. 2012/0209770 ("*'770 Application*")

37. Ex. 1017: U.S. Patent Pub. No. 2014/0121015 ("*Massing*")

38. Ex. 1018: U.S. Patent Pub. No. 2006/0058088 ("*Crawford*")

39. Ex. 1023: U.S. Patent Pub. No. 2012/0240203 ("*Kling*")

40. Ex. 1024: 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)

41. Ex. 1025: U.S. Patent No. 7,865,950 ("*Lipetz*")

42. Ex. 1027: Second Declaration of Sigurd Meldal

43. Ex. 1028: P. Traynor et al., "From Mobile Phones to Responsible Devices," Security Comm. Networks 2011, 4:719–726, (Wiley Online Library, August 28,2010)

44. Ex. 1029: Third Declaration of Sigurd Meldal, Dr. Scient

45. Ex. 1030: U.S. Patent Pub. No. 2013/0023241 ("*Lim*")

46. Ex. 1031: U.S. Patent No. 7,676,829 ("*Gui*")

47. Ex. 1032: Deposition Transcript of Patrick Traynor – May 13, 2024
(condensed)

48. I have also reviewed various other sources cited within this declaration.

49. In forming my opinions, I have considered the materials listed above and any documents cited in this declaration. I have also relied on my own education, knowledge, and experience in the relevant art.

50. I have also considered the understanding of a POSITA around the time of the invention the '376 Patent.

IV. LEGAL PRINCIPLES

51. I am not an attorney and will not offer opinions on the law.

52. In forming the analyses and conclusions expressed in my declaration, I have applied the legal principles described in the following paragraphs, which were provided to me by counsel for the Patent Owner.

A. Priority

53. I understand that a patent may claim the benefit of the filing day of an earlier filed application if the earlier filed application provides adequate disclosure of the patent's claims. I understand that the disclosure requirement is satisfied if a POSITA could clearly conclude that the inventor invented the claimed subject matter as of the earlier filing date sought. I understand that the earlier filed

application does not need to describe the claimed subject matter in precisely the same terms as found in the claims at issue.

B. Obviousness

54. I have been informed that a patent claim is invalid as “obvious” under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a person of ordinary skill in the art at the time of the alleged invention (“POSITA”), taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include “long felt need” for the claimed invention, commercial success attributable to the claimed invention, unexpected results of the claimed invention, skepticism of others, failure by others to achieve the claimed invention, and “copying” of the claimed invention by others.

55. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason that would have prompted a POSITA to modify the single prior art reference, or combine two or more references, in a manner that provides the elements of the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference(s) themselves, the

knowledge or “common sense” of a POSITA, or from the nature of the problem to be solved, and this reason may be explicit or implicit from the prior art as a whole. I have been informed that, under the law, the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

C. Analogous Art

56. I understand that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). *See* MPEP § 2141.01(A). I understand that “‘same field of endeavor’ and ‘reasonably pertinent’ are two separate tests for establishing analogous art; it is not necessary for a reference to fulfill both tests in order to qualify as analogous art.” MPEP § 2141.01(A).

57. When determining whether the “relevant field of endeavor” test is met, the one should consider “explanations of the invention’s subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.” *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019); MPEP § 2141.01(A). “When determining whether a prior art reference meets the

‘same field of endeavor’ test for the analogous art, the primary focus is on what the reference discloses.” *Airbus S.A.S.*, 941 F.3d at 1380; MPEP § 2141.01(A).

58. To determine if a reference is “reasonably pertinent,” one should “consider the problem faced by the inventor, as reflected - either explicitly or implicitly - in the specification. In order for a reference to be ‘reasonably pertinent’ to the problem, it must ‘logically [] have commended itself to an inventor's attention in considering his problem.’” *In re ICON Health and Fitness, Inc.*, 496 F.3d 1374, 1379-80 (Fed. Cir. 2007); MPEP § 2141.01(A). “An inventor is not expected to have been aware of all prior art outside of the field of endeavor.” *Airbus*, 41 F.3d at 1380-82; MPEP § 2141.01(A). “A reference outside of the field of endeavor is reasonably pertinent if a person of ordinary skill would have consulted it and applied its teachings when faced with the problem that the inventor was trying to solve.” *Airbus*, 41 F.3d at 1380-82; MPEP § 2141.01(A).

D. Motivation to Combine References

59. When relying upon multiple references to attempt to show obviousness, the challenger must explain why one of ordinary skill in the art would be motivated to combine or modify the references and what would have provided the basis of a reasonable expectation of success. *See Tris Pharma, Inc. v. Actavis Lab'ys FL, Inc.*, No. 2021-1495, 2022 WL 2525318, at *4 (Fed. Cir. July 7, 2022). As the Supreme Court noted in *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007),

there must be “a reason” for a skilled artisan “to combine the elements in the way the claimed new invention does”). *Tris Pharma, Inc.*, 2022 WL 2525318, at *4.

E. Written Description

60. “The test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date.” *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010)

F. Indefiniteness

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

G. Claim Construction

62. I understand that claim construction is a matter that will be decided by the Board presiding over this IPR. I understand that the relevant inquiry in claim construction is the question of how a POSITA would have understood the claim terms at the time of the earliest priority date, in light of the patent specification, the prosecution history, and any other relevant intrinsic and extrinsic evidence.

V. PERSON OF ORDINARY SKILL IN THE ART

63. All of the opinions that I express here have been made from the standpoint of a person of ordinary skill in the art at the time of the invention of the '376 Patent, which I may refer to as a "POSITA."

64. I understand that, for the purposes of this proceeding, the '376 patent is entitled to a priority date of no later than July 28, 2014.

65. I understand that the Petitioner has proposed that a POSITA at about the priority date of the '376 patent would have had "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." Ex. 1002, ¶31.

66. I understand that in the Institution Decision the Board adopted Petitioner's statement of the level of ordinary skill in the art. I further understand the Patent Owner did not file a substantive response to the Petition, and therefore Board was not presented with an alternative hypothetical level of ordinary skill.

67. For the purposes of this proceeding, I mostly agree with Petitioner's proposed level of skill with some clarification and adjustment. In my opinion, a POSITA at the relevant time frame 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 security and/or network design and security. Petitioner's proposed catchall statement "or other relevant industry experience" is vague and unhelpful.

68. At the relevant time frame, I was a person of more than ordinary skill in the art during the relevant timeframe. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

VI. WRITTEN DESCRIPTION

A. WRITTEN DESCRIPTION SUPPORT

69. I have reviewed the proposed Substitute Claims 26-41 attached to Patent Owner's Motion to Amend. Using the limitations of the Substitute Claims, I have prepared a table showing each limitation of the Substitute Claims as well as the paragraphs (and/or page numbers) to the excerpts from Dr. Rubin's Patent Application No. 14/444,995 supporting the Substitute Claims. The text highlighted in **bold** reflects the proposed changes made to the Substitute Claims in the Revised Motion to Amend.

Claim	Claim Element of Substitute Claim	'995 App.
[26Pre]	A method for protecting information by transmitting information to multiple electronic devices, the method comprising:	¶2; ¶18-19; ¶20 ¶23-25; ¶55; ¶61; ¶63-65, ¶78; ¶81, ¶83, ¶93

[26a]	electronically storing a set of information at a server;	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶89-90;
[26b]	identifying a first subset of the information and identifying a second subset of the information, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	¶23-28; ¶38
[26c]	determining at the server whether both a first device in possession of and being directly operated by a first user and a second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not authentication information specific to a device at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device.	Fig. 10; ¶26; ¶33; ¶75; ¶83; ¶89; ¶90; ¶92
[26d]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device thereby protecting the second subset of the information not transmitted to the	Abstract, Fig. 2; Fig. 4; Fig. 5; Fig. 6; Fig. 7; Fig. 9; Fig. 10; ¶20; ¶23-29 ¶33-34; ¶55; ¶58; ¶61; ¶63-65; ¶78; ¶81; ¶82; ¶83; ¶93

	first device from potential malware on the first device.	
[27]	The method of claim <u>26</u> , further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.	¶24; ¶38-39; ¶45; ¶48
[28]	The method of claim <u>26</u> , wherein	
[28a]	the first subset of the information comprises non-sensitive information; and	¶30-32
[28b]	the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.	¶23-26; ¶29; ¶30-32; ¶35; ¶57; ¶63; ¶78; ¶82
[29]	The method of claim <u>26</u> , wherein the information received at the second device is more sensitive than the information received at the first device.	¶24; ¶30-32; ¶35; ¶57; ¶78;
[30]	The method of claim <u>28</u> , 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.	¶33; Claim 5 (p.28)
[31]	The method of claim <u>26</u> , wherein the transmitting a first subset of the information to the first device from the server and transmitting a second subset of the information to the second device from the server are executed over independent electronic communications networks.	Fig. 5; Fig. 6; ¶27; ¶29; ¶33; ¶35;
[32]	The method of claim <u>26</u> , further comprising displaying a graphical	¶45; ¶48;

Third Decl. ISO Patent Owner's Reply
Case No. IPR2023-00376

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

	play the game, and wherein in the game server communicates sensitive information to the second electronic device so that sensitive information can be presented to a user.	
[38]	The method of claim <u>37</u> , wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.	Fig. 2; Fig. 4; Fig. 5; Fig. 6; ¶25-26; ¶31; ¶45; ¶48
[39]	The method of claim <u>26</u> , further comprising electronically storing at the server a parameter indicating whether subsets of the information are to be divided between two or more devices.	¶25-26; ¶31; ¶33-34; ¶35
[40]	The method of claim <u>26</u> , wherein the first and second subsets of information are application-specific, and wherein the first and second subsets of information derive from functions within a specific application.	¶20-23; ¶55 ¶57; ¶77-78
[41pre]	A system for protecting information by transmitting information to multiple electronic devices, the system comprising:	¶2; ¶18-19; ¶20 ¶23-25; ¶55; ¶61; ¶63-65, ¶78; ¶81, ¶83, ¶93
[41a]	an electronic data store configured for electronically storing a set of information at a server, wherein the first and second subsets of information are generated by the same application at the server and are specific to that application;	Fig. 5; Fig. 6; ¶25; ¶38; ¶39; ¶89-90
[41b]	a processor device programmed for:	¶81; ¶98 ¶¶101-102
[41c]	identifying a first subset of the information and identifying a second subset of the information;	¶23-28; ¶38
[41d]	determining at the server whether both a first device in possession of and being directly operated by a first user and a	Fig. 10; ¶26; ¶33; ¶75;

	second device also in possession of and being directly operated by the first user are accessible over at least one electronic communications network based on the first user being logged into the application using application specific authentication information that is not authentication information specific to a device at both the first and second devices wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device;	¶83; ¶89; ¶90; ¶92
[41e]	if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device.	Abstract, Fig 2; Fig. 4; Fig. 5; Fig. 6; Fig. 7; Fig. 9; Fig. 10; ¶20; ¶23-29 ¶33-34; ¶55; ¶58; ¶61; ¶63-65; ¶78; ¶81; ¶82; ¶83; ¶93

B. RESPONSE TO PETITIONER'S WRITTEN DESCRIPTION ARGUMENTS

70. *Claims 26 and 41.* Petitioner argues claims 26, 28 and 41 lack written description support. As discussed below, I respectfully disagree.

71. Petitioner argues claims 26 and 41 lack written description support because the specification does not disclose the use of application specific

authentication information that is “not authentication information specific to a device at **both** the first and second devices.” Pet. Opp. at 1.

72. The specification conveys that Dr. Rubin was in possession of the claimed subject matter. The patent teaches this exact limitation with respect to teaching a first device and a second device that each use non-device specific authentication information (e.g., passwords) to login to the application. Ex. 2005 ¶90 (“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.”). Indeed, the '376 patent only discloses using a password (i.e., authentication information that is not device specific) with the first device. Ex. 2005 ¶¶ 74, 90.

73. Dr. Rubin also teaches in the specification that use of device specific authentication, in some circumstances, may not be desirable because use of such an authentication scheme limits the user to a specific device. Ex. 2005, ¶92. In particular, Dr. Rubin states “[i]f 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.” *Id.* The concept stated by Dr. Rubin is straightforward,

known by POSITA in 2014 and frankly common sense. Use of authentication information that is not device specific will allow the user to use any device that can execute the applicable software application. This is a known concept to a POSITA, and as described in the '376 Patent, the concept applies to all devices, and whether such device is used as the first device or second device in Dr. Rubin's '376 Patent.

74. Dr. Rubin introduces the invention as including an invention that “includes an architecture . . . [with] a first device, which can be a computer, a tablet, a smartphone or other electronic device and a second device, such as a computer, tablet, smartphone or another type of electronic device. **Any combination of electronic devices can be used.**” (emphasis added). Ex. 2005, ¶19.

75. In light of the foregoing, it is my opinion '376 Patent specification reasonably conveys to those skilled in the art that Dr. Rubin had possession of the claimed subject matter as of the '376 Patent filing date.

76. **Claim 28.** Petitioner argues claim 28 lacks written description support because “nothing in the specification teaches that the sensitive information that is transmitted to the second device cannot ever be shared, disclosed, or communicated to any other device or person.” I respectfully disagree.

77. Dr. Rubin's specification teaches in a number of instances that “sensitive information is only shared with the second device.” For example, Dr. Rubin describes an online gaming example of Texas Holdem where “the game

server does not communicate certain sensitive information (such as, for example, the user's hole cards) to the first device. . . . Accordingly, because the sensitive information is not displayed or transmitted to the first device, an attacker using malware cannot gain access to the sensitive information." Ex. 2005 ¶23. Dr. Rubin further teaches "[e]verything that is known and displayed on the first device is considered to be public information, *and the only private, sensitive information exists on or is transmitted to a separate electronic device.*" Ex. 2005 ¶ 24 (emphasis added); *see also* Ex. 2005 ¶¶ 25-29.

78. Petitioner attempts to argue that only sharing sensitive information with the second device is specifically contradicted by the specification. Pet. Opp. at 2. In particular, Petitioner relies on Dr. Meldal's declaration where Dr. Meldal's cites the disclosure in Dr. Rubin's specification where the "hidden hole cards can be sent to the first device, so that they can be stored in hand histories that are kept on the first device." Ex. 1029, ¶12. This disclosure, however, is perfectly consistent with revised claim 28 because the game is over when the hole cards are transmitted to the first device, and the hole cards no longer constitute "sensitive information."

79. In my opinion, the '376 Patent specification reasonably conveys to those skilled in the art that Dr. Rubin had possession of the claimed subject matter as of the '376 Patent filing date.

VII. RESPONSE TO PETITIONER'S INDEFINITENESS ARGUMENTS

80. Petitioner contends the phrase “the information displayed on the respective devices” in claims 32 and 35 is indefinite because its scope cannot be determined. I respectfully disagree.

81. The specification discloses using a graphical indicator to link separate computing devices in the context of an online application (for example, online poker). Ex. 2005, ¶26. For example, Fig. 2 illustrate a user playing online poker where online poker table appears on the user's first device and the user's hole cards are sent to the second device. 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 ¶26. The specification further discloses using a special border or color scheme around a poker table displayed on the first device to help link the hole cards displayed on the user's second device. Ex. 2005 ¶45.

82. Additionally, original claim 10 which is considered part of the original written description claimed the method of claim 1, “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.” Ex. 2005-029. Original claim 11 further claimed the method of claim 10, “wherein the information linked at the second device comprises hole cards and the information linked at the first device comprises community cards in a hand in a game of poker.” Ex. 2005-029.

83. The foregoing disclosures are more than sufficient to allow POSITA to reasonably understand the boundaries of claims 32 and 35. In particular, it is obvious to a POSITA that “the information displayed on the respective devices” refers to the online application, such as online poker or banking, which is the object of Dr. Rubin’s invention. Figure 2 provides an example of a graphical identifier on the first and second device indicating a link between the information displayed on the respective devices, which in the Figure 2 embodiment represents the online poker table and the user’s hole cards.

**VIII. RESPONSE TO PETITIONER’S ARGUMENT THAT “THEREBY”
CLAUSE IS NON-LIMITING.**

84. In my opinion, the “thereby” clause of claim 26[d] and 41[e] adds to the patentability of the claims. The claims require that a second subset of information is sent by the application to only the second device. This isolation of information provides protection to the second subset of information because it is not exposed to malware that has potentially compromised the first device.

85. Absence of the “thereby” clause could technically allow a system to perform the steps of the ’376 patent but not protect the second subset of information sent the second device by, for example, allowing the first device to access the second device, or allowing the first device broad access to the application at the server. The steps of Dr. Rubin’s claims are meant, in part, to create isolation between the information sent to the first and second devices, but if the system

undermines the isolation by other means then the invention is not achieved. Dr.

Rubin's addition of the "thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device" makes it a requirement that the system establish isolation of the second subset of information not transmitted to the first device from potential malware on the first device.

Accordingly, in my opinion this limitations contributes to the patentability of claims 26 and 41.

IX. PETITIONER'S ZHA GROUNDS

86. *Zha* does not disclose the authentication requirements of substitute claim 26, limitation [c].

87. *Zha* discloses logging into the application program at each terminal, whether a desktop, laptop or cellphone. Ex. 1004, Col.12:51-56. However, *Zha* does not disclose any method of authentication. Moreover, *Zha* teaches that where the application program is a microblog, the users three devices – desktop, laptop and cellphone -- can all login to the microblog with "one microblog account." Ex. 1004, Col.6:56-61. Further, *Zha* teaches that once logged, any terminal can request and be assigned access to any functional interface. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48.

88. Petition relies on *Lipetz*, *Kling*, and a new reference, U.S. Patent No. 7,676,829 ("*Gui*") to claim that a POSITA would have been motivated to combine

these references with *Zha*, or modify *Zha* based on a POSITA's general knowledge from these references. I disagree for several reasons. First, neither *Lipetz*, *Kling* or *Gui* disclose using two different passwords to authenticate the first and second device as claimed in Substitute Claim limitation 26[c]. Second, there is no motivation to combine any of these three references with *Zha* even if they did disclose using application specific authentication information that is not device specific and that is different for the both devices.

89. ***Kling***. *Kling* does not disclose using application specific authentication information that is not authentication information specific to a device at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application specific authentication information used on the second device. *Kling* discloses using device specific authentication information for logging into the second device. Ex. 1023 ¶17. Further, *Kling* does not disclose using a different password for logging into ***the application*** on the second device. Ex. 1023 ¶18.

90. Petitioner tries to argue that *Kling*'s reference to logging into the mobile device "ideally using a different password" is actually a reference to logging into the application but paragraph 17 of *Kling* shows that *Kling* does not use "mobile device" and "application" interchangeably. *Kling* identifies a cell phone as a mobile device. Ex. 1023 ¶17 ("The secondary authentication request may be sent to

a mobile device *such as a cell phone*.”). *Kling* further discloses that the mobile device may “*open up a Web browser* or invoke *a specialized mobile banking app* upon receipt of the server notification.” (emphasis added). *Kling*’s reference to mobile device opening a web browser or invoking a specialized mobile banking app demonstrates logging into *Kling*’s “mobile device” is not synonymous with logging into the application which the claims require. In sum, *Kling* fails to disclose using a different application specific authentication information for the first and second devices.

91. Even if *Kling* disclosed using two different passwords to authenticate, there’s no motivation to combine with *Zha*. As discussed above, *Zha* permits any terminal (desktop, laptop, cellphone) to access any functional interface of the application program. Attempting to protect the second subset of information not sent to the first device – here according to Petitioner the functional interfaces of either the microblog home page, game interface or private messaging interface – makes no sense because the first device can simply change access permission and request access to any of the three functional interfaces.

92. ***Lipetz***. The *Lipetz* reference discloses a software security strategy of assigning a user multiple passwords that correspond with multiple security levels within an application. Ex. 1025, Col.1:6-10 (Background of the Invention). In *Lipetz* online banking embodiment, a user can receive multiple passwords when

logging into the banking application that correspond with different levels of access. For example, for a banking site user who is the owner of the account, under *Lipetz*, he or she can “employ a highly restricted password permitting check writing, fund transfers and changing personal information, an additional highly restricted, lower priority password is associated with the same username but has fewer privileges granted by the owner of that username for use by a designee.” Ex. 1025, Col.6:10-14.

93. *Lipetz* disclosure of using different passwords within a single application on a single device is for entirely different reasons than the use of two different passwords in '376 Patent, and addresses and entirely different concerns. Further, *Lipetz* disclosure of using two different passwords does not teach or disclose using two different passwords to log into the application on two different devices simultaneously. *Lipetz* discloses using one password at a time with one application on one device. A user will enter a new different password on the same device if the user wants to change their level of security access. Ex. 1025, Col. 8:52-62. *Lipetz* does not teach or suggest a user could benefit from using two different passwords simultaneously in the same online session.

94. Combining *Lipetz* with *Zha* would only make sense if *Zha* already required two different passwords on a single device to access the different functional interfaces for heightened security. *Lipetz* discloses a software security

strategy for assigning a user multiple passwords that correspond with multiple security levels within an application on a single device. Ex. 1025, Col.1:6-10, 6:10-14. A user will enter a new different password on the same device if the user wants to change their level of security access. *Id.*; Ex. 1025, Col. 8:52-62. Petitioner argues a POSITA would have been motivated to enhance *Zha* against malware by adding two different passwords on the two devices. But *Zha*'s microblog is already fully accessible by one device at any time using a single password. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48. A POSITA would not be motivated to add a second different password on a second device to access *Zha*'s chat feature when the user could access the same chat feature on their first device with the same password. This is not logical and just hindsight reasoning by Petitioner to try and combine *Lipetz* with *Zha*.

95. The '376 Patent is fundamentally about using two different devices simultaneously with an online application to enhance the security. *Lipetz* multiple password system still exposes all the information shared with the first device to malware potentially on the first device. *Lipetz* teaches using a different passwords with different levels of security, but at each level, all the information is shared with the first device and potentially exposed to malware.

96. **Gui.** Gui fails as a reference because its entire authentication is carried out by an authentication system that is independent of the application the user is

accessing. Ex. 1031, Col.7:27-32. As *Gui* explains, the “authentication system” is independent of “service” which the user is seeking to access. Ex. 1031, Col.7:27-32. The authentication system contracts with a number of systems to provide authentication, and the authentication system is responsible for maintaining all of various credentials associated with a user for the different systems. Ex. 1031, Col.8:15-26. Any of the user’s authentication credentials for the various systems can be invoked by the user to authenticate with the authentication system. Ex. 1031, Col.2:30-53.

97. *Gui* explains that the actual service that the user is seeking to gain access to “is typically unaware of the credential that was supplied by the user to the authentication system 210.” Ex. 1031, Col.7:57-60. Substitute claims 26 and 41 both require that “the server” running “the application” makes the determination of whether the first and second devices are in possession of the user based on the user being logged into the “application using application specific authentication information that is not authentication information specific to a device” and the authentication information is different for each device. *Gui* authentication system issues a “user profile and/or ticket” to the users device which is in turn provided to the service for authentication. In *Gui*, the server running the application (the “service”) does not know what type of authentication credentials were supplied to the authentication system. Similarly, applying *Gui* to *Zha*, the server would also

not know whether the authentication information used to login to two separate devices was different because the authentication system does not convey this information to the service. Ex. 1031, Col.7:57-60.

98. *Gui*'s authentication system also does not address the security benefits Substitute Claims 26 and 41 achieve by **requiring** two different passwords.

Applying *Gui*'s system to *Zha*, a user allowed to use the exact same password on the first device and second device to access the functional interfaces of *Zha*'s microblog. Accordingly, if the first device has been compromised by malware then the attacker can simply use the same password to log into *Zha*'s microblog on the second device. As Dr. Rubin explains in the '376 Patent, the benefit of requiring two different passwords protects against this very scenario. Ex. 2005 ¶ 90.

99. The foregoing example of the attacker compromising the first device, also underscores why it makes no sense for *Zha* to add two different passwords when logging in via a second device. Any user that gains access to *Zha*'s microblog on the first device has access all of the functional interfaces of *Zha*'s microblog.

100. In summary, *Gui*, *Kling* and *Lipetz* do not disclose using application specific authentication information that is not authentication information specific to a device at both the first and second devices, wherein the application specific authentication information used on the first device is different from the application

specific authentication information used on the second device whether for purposes of combining with *Zha*, or for establishing the general knowledge of a POSITA prior to the '376 Patent. Further, combining Gui's authentication system with *Zha* makes Substitute Claim limitation 26[c] "determining at the server" impossible because it is the "authorization system" that performs the authentication and shields "the server" running the application from knowing the authentication information used, and whether it was different for each device.

1. *Zha* Fails to Disclose the Preamble and of Substitute Claim Limitation [d].

101. The preamble provides that the method of Substitute Claim 26 is for "protecting information." Limitation [d] in the body of the claim was modified to add "thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first."

102. *Zha* does not meet either of these limitations. First, *Zha* does not protect information by transmitting information to multiple devices. *Zha* does not disclose protecting information at all, but more importantly, *Zha* teaches sharing that same information with the first device. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48.

Second, *Zha* does not disclose protecting the second subset of the information not transmitted to the first device from potential malware on the first device. *Zha* teaches providing the first device with access to all the same information available on the second device. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48.

103. Petitioner tries to suggest that a *Zha* meets these limitations by arguing a user could configure *Zha* to have the private messages sent to their cellphone and thus protect that information from potential malware on their desktop. Petitioner ignores the essential aspect of *Zha* which is that any terminal in *Zha* (the desktop, laptop and cellphone) can request access to any of the functional interfaces of *Zha*'s microblog. Thus, Petitioner is correct that a user could configure *Zha* so that the private messaging interface is provided to the cellphone when the user logs into *Zha*'s microblog on their cellphone. However, *Zha* discloses over and over that the user of the desktop can similarly request access to the private messaging interface. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48. An attacker that gains access to *Zha*'s first device, whether the desktop, laptop and cellphone, gains access to all of the functional interfaces of the microblog.

104. For this reason, *Zha* does not disclose "protecting information" from the preamble or "thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first device" from Substitute Claim limitation 26[d].

2. *Zha* Fails to Disclose Substitute Claim 27.

105. Substitute Claim 27 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 27.

3. *Zha* Fails to Disclose Substitute Claim 28[b].

106. Substitute Claim 28 states:

The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.

107. I understand that the Board in its Preliminary Guidance has given the term “Sensitive Information” its ordinary and customary meaning as would have been understood by a POSITA. PG at 20, Ex. 3002.

108. I further understand that Dr. Rubin has further narrowed Substitute Claim 28 by adding the requiring that the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device. As I note in Section VI above, there is substantial written description support in the '376 Patent specification for this added limitation.

109. I understand that the Board, based on its Preliminary Guidance, is persuaded that *Zha*’s private messages meet the definition of “sensitive information.” However, Substitute Claim 28 now further requires that sensitive information is only shared with the second device. *Zha*’s privates messages by definition cannot meet this limitation because they are messages between individuals and requires sharing the sensitive information beyond the second device. Moreover, any device in *Zha* can access *Zha*’s private messages, thus *Zha* fails to teach or disclose only sharing sensitive information with the second device.

110. I understand Petitioner makes two arguments as to why it contends *Zha* still discloses this limitation. Pet. Opp. at 16-17. Petitioner first argues that distinguishing *Zha* for disclosing private messages between users contradicts every embodiment in the '376 Patent. In particular, Petitioner argues the '376 Patent's "hole cards" are shared with every game participant. Pet. Opp. at 16-17. Petitioner is incorrect. The '376 Patent only discloses the "hole cards" once they no longer constitute "sensitive information." Petitioner further argues that the '376 Patent teaches "sharing" sensitive information beyond the second device (bank transaction information and health information), but Petitioner is incorrect. The specification teaches sharing the sensitive information generated by the application at the server only with the second device. Petitioner fails to cite any examples in the specification where the '376 Patent teaches "sharing" sensitive information beyond the second device.

111. Petitioner's second argument is that *Zha* only shares all the microblog interfaces in the *Zha* "single device" embodiment. This argument is incorrect and a distraction because *Zha* only discloses two device embodiments. As noted in the "Summary," *Zha* discloses a method for "displaying an interface" which includes "determining a first terminal and a second terminal." Ex. 1004, Col.1:50-55. Further, *Zha* discloses a system for "displaying an interface" with "at least two terminals according to any of the foregoing possible implementations." Ex. 1004,

Col. 2:54-58. It cannot be disputed that *Zha* only discloses two device embodiments and that in any of these embodiments, any of the “at least two terminals” can request access to any of the functional interfaces of *Zha*’s microblog. Ex. 1004, Col.14:6-12, 15:56-58, 16:37-48. Accordingly, *Zha* teaches away from only sharing sensitive information with the second device because *Zha* discloses sharing its private message interface with any of the at least two terminals.

4. *Zha* Fails to Disclose Substitute Claim 29.

112. Substitute Claim 29 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 29.

5. *Zha* Fails to Disclose Substitute Claim 30.

113. Substitute Claim 30 depends from Substitute Claim 28, and Substitute Claim 28 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26 and 28, *Zha* fails to disclose the limitations of Substitute Claim 30.

6. *Zha* Fails to Disclose Substitute Claim 31.

114. Substitute Claim 31 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 31.

7. *Zha* Fails to Disclose Substitute Claim 32.

115. Substitute Claim 32 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 32.

8. *Zha* Fails to Disclose Substitute Claim 34.

116. Substitute Claim 34 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 34.

9. *Zha* Fails to Disclose Substitute Claim 36.

117. Substitute Claim 36 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 36.

10. *Zha* Fails to Disclose Substitute Claim 37.

118. Substitute Claim 37 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 37.

11. *Zha* Fails to Disclose Substitute Claim 39.

119. Substitute Claim 39 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 39.

12. *Zha* Fails to Disclose Substitute Claim 40.

120. Substitute Claim 40 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 40.

13. *Zha* Fails to Disclose Substitute Claim 41.

121. Substitute Claim 41 is essentially identical to Substitute Claim 26 except that the Substitute Claim 41 is presented as a “[a] system for protecting information by transmitting information to multiple electronic devices.”

122. Substitute Claim limitation 41[d] corresponds with Substitute Claim limitation 26[c], and Substitute Claim limitation 41[e] corresponds with Substitute Claim limitation 26[e].

123. For the reasons *Zha* does not disclose the Substitute Claim limitation 26[c] set forth above in paragraphs 91-103, *Zha* also does not disclose the Substitute Claim limitation 41[d].

X. PETITIONER'S *KLING* GROUNDS

124. I have reviewed the proposed Substitute Claims in comparison with *Kling*. Ex. 2023. In my opinion the proposed substitute claims are patentable over *Kling*.

125. *Kling* was originally disclosed by Dr. Rubin to the patent office during prosecution of the '376 Patent. Fundamentally, *Kling* discloses a form of two-factor authentication which is the prior art Dr. Rubin's '376 Patent sought to

improve upon, and distinguish from. *Kling* describes itself as a form of two factor authentication. Ex. 1023, ¶7 (“[t]he overall security of this two-factor authentication is substantially higher than the original single factor authentication performed on a PC.”). As background, two-factor authentication is used to secure online applications by authenticating users, authorizing transactions, or notifying users of irregularities in their accounts. *See, e.g.*, Ex. 2003, ¶7. As Dr. Rubin’s ’376 Patent explains “in two-factor authentication, a user logs into a first device (e.g., a computer) and then uses a second device (e.g., a smartphone) as part of the authentication process.” *Id.* Once the two-factor authentication is complete the second device is no longer needed. *Id.*

126. It is common knowledge in the field of security that two-factor authentication does not protect the user from malware after the authentication is complete, or if the user’s first device is compromised by malware. Dr. Rubin’s ’376 Patent is fundamentally distinguishable from two-factor authentication scheme’s because the information a user wants to protect from compromise is exposed only to the second device, and only when the user is logged into both the first device and second device simultaneously.

127. *Kling* discloses what can be described as two-factor authentication for an online transaction carried out on the first device, plus an approval step sent to the second device. Ex. 2023, ¶18, Figs. 4, 5. *Kling*’s approval step sent to the

second device appears to be its advancement over basic two-factor authentication.

Kling helps to prevent malware on the first device from hijacking an online money transfer. However, unlike Dr. Rubin's '376 Patent, *Kling* scheme still exposes all of the user's banking information to potential malware on the first device. If the malware on the first device is directed towards capturing a user's confidential information, of any type, by simply observing and recording a user's activities, *Kling*'s two-factor "plus" authentication scheme offers no protections.

128. For example, *Kling*'s security scheme does nothing to protect from malware such as spyware¹ that secretly observes and records a user's activity to capture sensitive information which can later be sold on the dark web. *Kling* protects against the highjacking of the transaction but prior to the highjacking, spyware would have already learned the user's login, password, online bank, online bank accounts, online bank account balances and maybe even bank account numbers, all of which is recorded and sold.

129. Reviewing *Kling*'s Figure 5, if one simply modifies the Malware (512) to any common type of spyware that surreptitiously records a user's activity on their device (rather than malware that specifically attempts to highjack a

¹ Kaspersky.com provides a useful description of spyware at <https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>.

transaction), the malware would capture all of user's confidential banking information on the first device. The only information not shared with the first device under *Kling* is the "click 'OK' or Cancel" step sent to the second device.

130. Dr. Rubin's '376 Patent is an advancement over *Kling* and similar two-factor authentication schemes because it calls for a very specific, but advantageous, authentication process on two devices simultaneously, and then sends the protected information only to the second device as the first device may be compromised by malware.

A. Analysis of *Kling*.

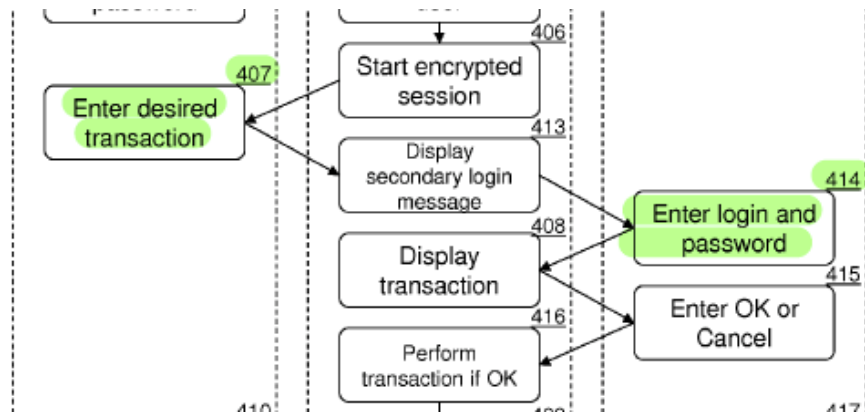
1. *Kling* fails to disclose the "if and only if" limitation 26[d].

131. The first portion of limitation 26[d] requires that **"if and only if both the first and second devices are determined to be accessible by the server, then:** transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server"

132. Petitioner's expert, Dr. Meldal, identified "enter desired transaction 407" as corresponding to the "first subset of information" in Substitute Claim 26. Ex. 2027, ¶87 ("First, the transaction web page information [Arrow #2] sent to user's PC for the user to 'enter desired transaction 407' corresponds to the claimed 'first subset of information.'"). Petitioner's expert, Dr. Meldal, further identified

“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” as corresponding to the “second subset of information.” Ex. 2027, ¶87.

133. Petitioner’s “first subset of information” is sent to the first device **before** both the first and second device are determined to be accessible by the server. As shown below, transmission of the first subset of information occurs at step 407, but the second device is not determined to be accessible by the server until step 414:



134. Substitute Claim 26 is explicit that “if and only if both the first and second devices are determined to be accessible by the server” then transmit the first and second subsets of information to the first and second devices. *Kling* does not follow the “if and only if” requirement but instead sends the first subset of information before the second device is authenticated. This is a fundamental distinction between performing two-factor authentication for purposes of securing an online transaction carried out principally on the first device disclosed in *Kling*,

versus Dr. Rubin's '376 Patent which requires simultaneous authentication on two devices during an online session and only sharing certain information with the second device to protect the information from malware that has potentially compromised the first device.

135. As a back-up argument for this missing element, Petitioner's expert argues the "if and only if" limitation would have been within a POSITA's general knowledge (citing to *Tsushima*), and a POSITA would have been motivated to combine this general knowledge to modify *Kling* to achieve the '376 Patent. See Ex. 1027, ¶¶100-104.

136. In my opinion, there is no motivation to modify *Kling* to add the "if and only if" limitation as purported general knowledge of a POSITA because such a modification would not change *Kling*'s security scheme before or after authentication. Further, modifying *Kling* to add the "if and only if" limitation would substantially disrupt *Kling*'s disclosed banking application that relies primarily on carrying out the activity on the first device while the second device is used solely to confirm transactions and then is disregarded.

137. First, there is no change to *Kling*'s security scheme by adding the "if and only if" limitation. As Dr. Meldal noted, "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.” Ex. 1027, ¶100. But even assuming a POSITA made this change, the rest of *Kling*’s security scheme would operate exactly the same.

138. Once the second device is authenticated on *Kling*, then the first subset of information (“enter desired transaction 407”) is sent to the first device (PC), and the second subset of information (“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”) is sent to the second device. The transaction is either confirmed or cancelled by the second device and the results of the transaction are displayed on both devices. There is no enhancement of securing the transaction under *Kling* by adding the “if and only if” limitation and refraining from transmitting the first and second subset of information until both devices are authenticated.

139. And even if *Kling* was modified to add an “if and only if” limitation, *Kling* would still share the user confidential banking information with the first device. Ex. 1023, ¶14, ¶17-18 (describing making a transfer request to another account and receiving the results of the transaction). The only banking information under *Kling* not exposed to the first device is the “secondary authentication request” sent to the second device after authentication where the “user can choose to confirm or cancel this request 415 which will terminate the secondary session.” Ex. 1023, ¶¶17-18.

140. Not only would modifying *Kling* to add the “if and only if” limitation not improve *Kling*’s security scheme in any manner, but it would significantly disrupt *Kling*’s described online banking process. *Kling* discloses a user being able to gain access to their online banking application and at least initiate transactions before triggering a “secondary authentication request.” Ex. 1023, ¶17 (“Upon receiving the user’s transaction request the bank server may decide, based on a set of rules to invoke secondary authentication request 413.”). *Kling* then suggests such “rules” could take into account various factors “such as the transaction amount and type.” Ex. 1023, ¶17. However, modifying *Kling* to require authentication of both devices at the outset before the first and second subsets of information can be sent, means under *Kling* a user can no longer access their banking application at all without their second device, even if such access would not require a secondary authentication request under the banking application’s rules.

141. Petitioner’s expert, Dr. Meldal, suggested three possible reasons why a POSITA would be motivated to modify *Kling* to add the “if and only if” limitation.

Dr. Meldal states:

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. 1027, ¶ 102.

142. Dr. Meldal further states “*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*.” Ex. 1027, ¶103.

143. Each of these statements are conclusory and do not provide a reason why a POSITA would have been motivated to modify *Kling*. Meldal’s first statement merely notes the similarities between the structure of *Kling* and the ’376 Patent’s banking embodiment. He does not explain why modifying *Kling* to add the “if and only if” limitation would improve *Kling*’s security scheme in some way as to motivate a POSITA to make the modification. Dr. Meldal’s second statement that *Kling* is similarly concerned with malware in banking application and therefore a POSITA would be motivated to modify *Kling* fails no better. As I discussed above, modifying *Kling* to add the “if and only if” limitation does not change or improve *Kling*’s security scheme and actually disrupts *Kling*’s online banking application.

144. In sum, modifying *Kling* to add the “if and only if” limitation disrupts the operability of *Kling*’s disclosed online banking application while simultaneously doing nothing to improve *Kling*’s security scheme. Even with the “if and only if” modification, *Kling* would continue to expose all the confidential banking information to the first device. Based on the foregoing, it is my opinion a

POSITA would not be motivated to modify *Kling* to add the missing “if and only if” requirement of Substitute Claim limitation 26[d].

2. *Kling* in combination with *Lim* fails to disclose 26[d]

145. I understand that in Petitioner’s Opposition, Petitioner now contends that *Kling* in combination with *Lim* discloses 26[d] “if and only if.” I respectfully disagree. Moreover, a POSITA would not look to combine *Kling* with *Lim* to achieve the ’376 Patent.

146. Petitioner misreads *Lim* and what it discloses. Petitioner asserts that *Lim* discloses “a user using two different authentication mechanisms (two different “application specific authentication information”) from two different devices to access the application. Pet. Opp. at 22. This is incorrect. *Lim* discloses authentication using only the mobile device.

147. First, in *Lim* a user connects with a “service server 300” (i.e., an online banking application) using the “user terminal 50.” Ex. 1030 ¶ 28. The user begins the login process and the “service server 300 provides an authentication interface including an identifier to the user terminal 50.” *Id.* The authentication interface provided by the service server includes an identifier/password and an “identifier 60.” Ex. 1030 ¶ 29.

148. *Lim*’s “mobile terminal 100” captures the identifier 60 and then provides the identifier to the *Lim*’s “authentication system 200.” Ex. 1030 ¶¶ 30-35.

The “authentication system 200” then compares the identifier information provided by “mobile terminal 100” with the identifier information originally provided to “user terminal 50 by the “service server 300.” Ex. 1030 ¶ 38.

149. If the identifier information is valid, then:

[T]he authentication system 200 requests authentication information from the mobile terminal 100, and the mobile terminal 100 provides the authentication information to the authentication system 200, thereby performing a final authentication process.

Ex. 1030 ¶30.

150. What is clear from the above is that ALL the authentication is carried out by the second device delivering the “identifier” and providing the authentication information requested by “authentication system 200.”

151. *Lim* then states: “That is, in the present invention, ***the user terminal 50 itself that will connect with the service server 300 does not perform authentication.***” Ex. 1030 ¶ 43. *Lim* further explains that “[i]n the present invention, the user terminal 50 only displays an identifier on a monitor screen in the authentication process, but does not become a principal agent of the authentication.” Ex. 1030 ¶ 44.

152. Accordingly, Petitioner has misinterpreted *Lim* as disclosing a system where a user uses two different authentication mechanisms.

153. *Lim* has additional deficiencies. Similar to *Gui*, *Lim*'s authentication is carried out by a different server than the "service server 300" running the online application. Ex. 1030, ¶¶24, 27. This means the server performing the "determining" of Substitute Claim limitation 26[c] is not the same server running the application that generates the subset of information. Further, *Lim* specifically discloses the use of device specific authentication information for authenticating the "mobile device 100." Ex. 1030 ¶ 48 ("Here, the authentication information may be one or more of the phone number of the mobile terminal 100, a MAC address, USIM or SIM card information"). While *Lim* discloses use of non-device specific authentication information such as a username and password as one possible means for authenticating mobile device 100, *Lim* teaches away from limiting authentication information to information that is not device specific. Finally, because *Lim* only discloses authenticating on one device, if fails to disclose authenticating on two devices using two different passwords.

3. *Kling* fails to disclose elements of 26[c].

154. Substitute Claim limitation 26[c] provides that:

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

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

155. *Kling* does not disclose using “application specific authentication information that is not authentication information specific to a device at both the first and second devices.” *Kling* teaches the opposite. *Kling* discloses that the “secondary authentication request may be sent to a mobile device such as a cell phone that the user has previously registered with the bank server.” Ex. 2023, ¶17. By definition, *Kling*’s banking application is relying on specific device information to carry out the initial authentication of the second device.

156. I understand Substitute Claim limitation 26[c] has been specifically narrowed further to require application specific authentication information that is not authentication information specific to a device. This is supported by the specification of the ’376 Patent which teaches the enhanced value of not using device specific authentication information. Ex. 2005, ¶92. In particular, the ’376 Patent teaches that using device specific authentication information will limit the user to using only certain devices, rather than any device that contains the appropriate application software. Ex. 2005, ¶92. Notably, the ’376 Patent’s teaching regarding the non-use of device specific authentication information is directed towards the user experience and not improving security.

157. *Kling* also fails to disclose using different application specific authentication information on the first device and second device as characterized by Petitioner and Dr. Meldal.

158. In describing the secondary authentication request process, *Kling* states:

The secondary authentication request may be sent to a mobile device such as a cellphone 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.

[0018] *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. 2023, ¶¶17-18 (emphasis added).

159. Importantly, *Kling* discloses a user being prompted to “**log into the mobile device, ideally using a different password than on the PC.**” This disclosure does not teach or disclose logging into the application on the second device using application specific authentication information that is different between the two devices. *Kling* only suggests logging into the mobile device with a password that is different than the password on the PC. There is no teaching or suggestion that the password used to login to the online banking application on each device is different. The '376 Patent specifically teaches there are advantages

to requiring different authentication information for the two devices. In particular, if the same authentication information is used for both devices “then the attacker could conceivably connect to the server with an illegitimate second device and impersonate the user.” Ex. 2005, ¶90. By requiring login to the application on the two devices using different authentication information protects against this vulnerability. This is consistent with my prior testimony in this matter along with my existing publications.

160. As discussed previously, Petitioner argues that *Kling*'s reference to logging into the “mobile device” is synonymous with logging into the banking application. But as discussed above, *Kling* makes clear that mobile device and the banking application are separate. Ex. 1023 ¶17 (“The mobile device may . . . invoke a specialize mobile banking app upon receipt of the server notification.”). *Kling* discloses in figure 4 and figure 5 entering a “login and password” as part of a secondary login, but fails to disclose any further details about that process including whether the authentication information is different than the authentication information used in steps 404 and 504 of Figures 4 and 5, or whether the authentication information is not device specific.

161. As noted above, combining *Kling* with *Lim* does not disclose this limitation. *Lim* only discloses authenticating on a single device, “mobile device 100,” does not disclose using different authentication information on two devices,

and teaches away from using application specific authentication information that is not device specific.

162. In summary, the Substitute Claim limitation 26[c] requires the use of “application specific authentication information that is not authentication information specific to a device” and that is “different” for the two devices. *Kling* teaches using device specific authentication information as part of its secondary authentication scheme which is contrary the claim limitation. Further, *Kling* suggests using a different password for logging into the mobile device, but does not teach or suggest using a different password for logging into the application on the mobile device which is a specific teaching of the '376 Patent and requirement of Substitute Claim limitation 26[c]. *Kling* in combination with *Lim* does not fix any of the deficiencies outlined above.

4. *Kling* Fails to Disclose Substitute Claim Limitation 27.

163. Substitute Claim 27 depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claim 26, *Kling* fails to disclose the limitations of Substitute Claim 27.

5. *Kling* Fails to Disclose Substitute Claim Limitation 28[b].

164. Substitute Claim 28 states:

The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.

165. I understand that the Board in its Preliminary Guidance has given the term “Sensitive Information” its ordinary and customary meaning as would have been understood by a POSITA. PG at 20, Ex. 3002.

166. I further understand that Dr. Rubin has further narrowed Substitute Claim 28 by adding the requirement that the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device. As I note in Section VI above, there is substantial written description support in the '376 Patent specification for this added limitation.

167. Petitioner argues the “transaction confirmation web page information [Arrow #4]” comprises “sensitive information” and that “transaction confirmation web page information” is only shared with the user’s second device. Pet. Opp. 28.

168. This argument fails for obvious reasons. Assuming for sake of argument, *Kling*’s “desired transaction” shared with the second device is “sensitive information” that information has already been shared with the first device which is expressly prohibited by Substitute Claim limitation 28[b]. The requested transaction was generated by the first device. As noted above, Substitute Claim limitation 28[b] provides that “the sensitive information is only shared with the second device.”

169. In summary, *Kling* fails to disclose Substitute Claim limitation 28[b] because *Kling* does not disclose sensitive information sent to the second device as

part of the “second subset of information” that is only shared with the second device.

6. *Kling* Fails to Disclose Substitute Claim 29.

170. Substitute Claim 29 depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claim 26, *Kling* fails to disclose the limitations of Substitute Claim 29.

7. *Kling* Fails to Disclose Substitute Claim 30.

171. Substitute Claim 30 depends from Substitute Claim 28 which depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claims 26 and 28, *Kling* fails to disclose the limitations of Substitute Claim 30

172. Furthermore, claim 30 requires “determining if connectivity between the server and the second device has been disrupted; and providing a notification on the second device that the connectivity has been disrupted.” *Kling* is silent with respect to this limitation and therefore does not disclose it.

173. Petitioner argue that a POSITA would rely on their general knowledge to modify *Kling* to add this limitation. In my opinion, a POSITA would not be motivated to modify *Kling* to add this limitation. This is because *Kling*'s connectivity with the second device is only for the limited purpose of providing secondary authentication of a transaction carried out on the first device. Ex. 1023,

¶18 (stating “[t]he user can choose to confirm or cancel this request 415 which will terminate the secondary session.”). There is no advantage to *Kling* adding this limitation because, unlike the ’376 Patent, *Kling* does not invoke use of the second device beyond merely requesting authorizing of a transaction. *Kling*’s mobile device only connects momentarily to the server in order to authorize the requested transaction. In contrast, the ’376 Patent describes one embodiment of the online poker game requiring persistent connection throughout the game otherwise the player is folded out. Ex. 2005, ¶¶31-32.

8. *Kling* Fails to Disclose Substitute Claim 31.

174. Substitute Claim 31 depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claim 26, *Kling* fails to disclose the limitations of Substitute Claim 31.

9. *Kling* Fails to Disclose Substitute Claim 34.

175. Substitute Claim 34 depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claim 26, *Kling* fails to disclose the limitations of Substitute Claim 34.

10. *Kling* Fails to Disclose Substitute Claim 40.

176. Substitute Claim 40 depends from Substitute Claim 26. For the reasons *Kling* fails to disclose the limitations of Substitute Claim 26, *Kling* fails to disclose the limitations of Substitute Claim 40.

11. *Kling* Fails to Disclose Substitute Claim 41

177. Substitute Claim 41 is essentially identical to Substitute Claim 26 except that the Substitute Claim 41 is presented as a “[a] system for protecting information by transmitting information to multiple electronic devices.”

178. Substitute Claim limitation 41[d] corresponds with Substitute Claim limitation 26[c], and Substitute Claim limitation 41[e] corresponds with Substitute Claim limitation 26[e].

179. For the reasons *Kling* does not disclose the Substitute Claim limitation 26[c] and 26[d] set forth above in paragraphs ¶¶52-73, *Kling* also does not disclose the Substitute Claim limitation 41[d] and 41[e].

XI. PETITIONER’S TAKAHASHI GROUNDS

A. *Takahashi* Fails to Disclose Substitute Claim 26

1. *Takahashi* fails to disclose the authentication limitations of 26[c].

180. Substitute Claim 26[c] requires:

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

181. As discussed in my previous declaration, Substitute Claim 26 requires “determining at the server” if both devices are accessible based on “the first user **being logged into the application**” using application specific authentication information. *Takahashi* clearly discloses something different. In Figure 11, *Takahashi* plainly discloses an authentication process that occurs “after user logins.” Ex. 1007, Fig. 11. Similarly, paragraph 110 (describing Fig. 11) discloses “processing after a registered user (that is, a user whose ID is registered) logins to the game server 20.” Ex. 1007, ¶110. Similarly, in paragraph 14 (describing Fig. 12) *Takahashi* makes clear it is using the term “login” in its well understood meaning to a POSITA when the disclosure equated accessing the game server as the same thing as logging in. Ex. 1007, 114 (“an access is received to the game server 20 (that is, a user logins)”).

182. Petitioner contends that *Takahashi*’s disclosure of user logon before the *Takahashi* authentication steps means something other than its plain disclosure. Pet. Opp. 33. Petitioner suggests the disclosure of “login” does not mean what it says, and only relates to the first step of the user submitting their credentials. *Id.* This argument is contradicted by *Takahashi*’s later discloser describing Figure 12 that the users accessing of the game server is the same as the user logging in. Ex. 1007, ¶114. Thereafter, *Takahashi* begins execution of the steps described in Figure 12

which include sending first and second subsets of data to the first and second devices.

183. *Takahashi* fails to disclose Substitute Claim limitation 26[c] because *Takahashi* discloses authenticating the user after the user has logged in.

184. *Takahashi* also fails to disclose Substitute Claim limitation 26[c] because *Takahashi* specifically relies on device specific authentication information. Ex. 1007 ¶74 (“Identification information may be a serial number of the mobile terminal.”). The Board’s Preliminary Guidance found that “use of ‘identification information’ that is unique to each mobile terminal” appears to correspond with “application specific authentication information.” PG at 26. Substitute Claim limitation 26[c] now specifically excludes use of this type of device specific authentication information. Accordingly, *Takahashi* fails to disclose this limitation and instead teaches away from this claim limitation by explicitly calling for the use of device specific authentication information.

2. *Takahashi* Fails to Disclose the Preamble and of Substitute Claim Limitation [d].

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

malware on the first.” I understand that Petitioner contends these claim amendments are “non-limiting” and thus *Takahashi* does not have to disclose these limitations. I note, however, that Petitioner’s Opposition does not argue or contend that *Takahashi* discloses “protecting information” from the preamble or “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first” from Substitute Claim limitation 26[c].

186. Further, in my opinion, *Takahashi* does not disclose these limitations. First, *Takahashi* does not protect information by transmitting information to multiple devices. *Takahashi* does not disclose protecting information at all, but more importantly, *Takahashi* teaches sharing that same information with a single device. Second, *Takahashi* does not disclose protecting the second subset of the information not transmitted to the first device from potential malware on the first device. *Takahashi* teaches providing the first device with access to all the same information on the second device. In my opinion, *Takahashi* does not disclose the preamble or the revised limitation [d].

187. Petitioner’s expert, Dr. Meldal, argues that teachings of *Takahashi*’s two-device embodiments should be discounted or rendered a “nullity” because of other disclosed embodiments. Pet. Opp. at 33. Dr. Meldal states that “[e]ven if *Takahashi* teaches a single-device embodiment where all information is transmitted to a single device, I understand that prior art references are to be considered for all they teach to

a person of skill in the art.” Ex. 1029, ¶268. I agree, and the point is *Takahashi* teaches away from several key aspects of Substitute Claims 26 and 41. In particular, *Takahashi* teaches away from “thereby protecting the second subset of the information not transmitted to the first device from potential malware on the first” because *Takahashi* teaches that the second device can be removed from the game and all the information, including the purportedly “sensitive information” on the second device is collapsed into the first device.²

B. *Takahashi* Fails to Disclose Substitute Claim 27.

188. Substitute Claim 27 states:

The method of claim 26, further comprising transmitting at least a portion of the first subset of the information to the second device from the server only if both the first and second devices are determined to be accessible by the server.

189. *Takahashi* fails to disclose 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.

² Dr. Meldal argument that *Takahashi* sharing of all information with the first device is similar to embodiments in the '376 Patent does not help his position. Ex. 1029 ¶269. The embodiment Dr. Meldal refers to is unclaimed description of playing online poker on a single device and does not relate to any of the original claims of the '376 Patent, or any of the Substitute Claims which all claim use of two devices. Unlike *Takahashi*, when the second device is lost (for example, due to a poor connection), the '376 Patent describes a number of alternative that can be undertaken by the user to attempt to maintain security benefit of the '376 Patent, or the user can opt to proceed on one device but understanding they are no longer protected by the security benefits of the '376 Patent. Ex. 2005 ¶¶31, 33-34.

190. In particular, *Takahashi* discloses that in its two device embodiment, the information sent to the first and second devices is different:

- “In this case, the HTML data (second game data) transmitted to the main-terminal and the HTML data (first game data) transmitted to the sub-terminal are different each other.” Ex. 1007, ¶ 107.
- “The transmitted HTML data to the mobile terminal 10 is different from the one transmitted to the PC 12. Ex. 1007, ¶ 116.

191. Because Substitute Claim 27 requires that at least a portion of the first subset of information be sent to the second device, *Takahashi* fails to disclose this limitation.

192. Further, Substitute Claim 27 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 27.

C. *Takahashi* Fails to Disclose Substitute Claim 28[b].

193. Substitute Claim 28 states:

The method of claim 26, wherein the first subset of the information comprises non-sensitive information; and the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device.

194. I understand that the Board in its Preliminary Guidance has given the term “Sensitive Information” its ordinary and customary meaning as would have been understood by a POSITA. PG at 20, Ex. 3002.

195. I further understand that Dr. Rubin has further narrowed Substitute Claim 28 by adding the requiring that the second subset of the information comprises sensitive information and the sensitive information is only shared with the second device. As I note in Section VI above, there is substantial written description support in the '376 Patent specification for this added limitation.

196. *Takahashi* fails to disclose sending sensitive information to the second device. Petitioner argues that the user's "game results" could constitute (i.e., number of fish caught in Fig. 8) confidential information. Game results for a social fishing game meant to be played with friends does not meet the Board's construction of sensitive information. Further, there is no teaching in *Takahashi* that a user's game results is sensitive information. *Takahashi* simply notes that the "display" on the second device could be configured to be different then the display on the first device because in doing so "allows game entertainment to be enhanced." Ex. 1007, ¶ 120. There is simply nothing *Takahashi* to teach or suggest *Takahashi*'s game results are sensitive information as construed by the Board.

197. More importantly, *Takahashi* teaches away from disclosing sensitive information with only the second device (a requirement of Substitute Claim 28). The "game results" in *Takahashi*'s single device embodiment are by definition shared with the first device, otherwise how could the game be played. In *Takahashi* single device embodiment where a second device is added, the game results may

then be sent to the second device but only after they have been shared with the first device. For example, in Takashi the user may access the game via a single terminal where all the game information is delivered before adding a second terminal:

Note that there is a case in which a user starts *the game* by accessing first through a single communication terminal (mobile terminal 10, for example) and then accesses through the other communication terminal (PC 12, for example) as well in the middle of the game. In Such case, after recognizing that there is an access from the PC 12, the game server 20 rewrites the database server 30 such that status in which the mobile terminal 10 is identified as both main terminal and Sub-terminal, is changed to status in which the PC 12 is identified as main-terminal and the mobile terminal 10 as sub-terminal. The game server 20 then switches transmission destination of the HTML data for displaying a new web page from the mobile terminal 10 to the PC 12.

Ex. 1007, ¶120.

198. Finally, *Takahashi's* two device embodiments contemplate disconnecting the second device and continuing the game on the first device whereby any purported “sensitive information” such as “game results” is necessarily sent to the first device. Ex. 1007, ¶143, Fig. 20.

D. *Takahashi* Fails to Disclose Substitute Claim 29.

199. Substitute Claim 29 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 29.

E. *Takahashi* Fails to Disclose Substitute Claim 30.

200. Substitute Claim 30 depends from Substitute Claim 26. For the reasons *Zha* fails to disclose the limitations of Substitute Claim 26, *Zha* fails to disclose the limitations of Substitute Claim 30.

F. *Takahashi* Fails to Disclose Substitute Claim 31.

201. Substitute Claim 31 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 31.

G. *Takahashi* Fails to Disclose Substitute Claim 32.

202. Substitute Claim 32 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 32.

H. *Takahashi* Fails to Disclose Substitute Claim 33.

203. Substitute Claim 33 states:

The method of claim 26, wherein the information received at the second device is a user's private cards in an online card game.

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

205. Furthermore, Substitute Claim 33 depends from Substitute Claim 26.

For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 33.

I. *Takahashi* Fails to Disclose Substitute Claim 34.

206. Substitute Claim 34 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 34.

J. *Takahashi* Fails to Disclose Substitute Claim 35.

207. Substitute Claim 35 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 35.

K. *Takahashi* Fails to Disclose Substitute Claim 36.

208. Substitute Claim 36 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 36.

L. *Takahashi* Fails to Disclose Substitute Claim 37.

209. Substitute Claim 37 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 37.

M. *Takahashi* Fails to Disclose Substitute Claim 38.

210. Substitute Claim 38 states:

The method of claim 37, wherein the online game is poker and wherein the information that is communicated to the second device includes hole cards.

211. *Takahashi* does not disclose this limitation, and Petitioner provides no analysis or evidence that *Takahashi* in combination with any other reference discloses the online game is poker and wherein the information that is communicated to the second device includes hole cards.

212. Further, Substitute Claim 38 depends from Substitute Claim 37 which depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 38.

N. *Takahashi* Fails to Disclose Substitute Claim 39.

213. Substitute Claim 39 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 39.

O. *Takahashi* Fails to Disclose Substitute Claim 40.

214. Substitute Claim 40 depends from Substitute Claim 26. For the reasons *Takahashi* fails to disclose the limitations of Substitute Claim 26, *Takahashi* fails to disclose the limitations of Substitute Claim 40.

P. *Takahashi* Fails to Disclose Substitute Claim 41.

215. Substitute Claim 41 is essentially identical to Substitute Claim 26 except that the Substitute Claim 41 is presented as a “[a] system for protecting information by transmitting information to multiple electronic devices.”.

216. Substitute Claim limitation 41[md] corresponds with Substitute Claim limitation 26[c], and Substitute Claim limitation 41[e] corresponds with Substitute Claim limitation 26[e].

217. For the reasons *Takahashi* does not disclose the Substitute Claim limitation 26[c] and 26[d] set forth above, *Takahashi* also does not disclose the Substitute Claim limitation 41[d] and 41[e].

Q. *Takahashi* Combined with *Gui* Does Not Cure *Takahashi*'s Deficiencies

218. Petitioner argues a POSITA would have been motivated to combine *Takahashi* with *Gui*'s authentication system to add the implementation of different passwords on different devices. I respectfully disagree.

219. First, as discussed above, *Gui* authentication system *Gui* fails as a reference because its “authentication system” is independent of “service” which the user is seeking to access. Ex. 1031, Col.7:27-32. The authentication system contracts with a number of systems to provide authentication, and the authentication system is responsible for maintaining all of various credentials associated with a user for the different systems. Ex. 1031, Col.8:15-26. Any of the user's

authentication credentials for the various systems can be invoked by the user to authenticate with the authentication system. Ex. 1031, Col.2:30-54.

220. *Gui* explains that the actual service that the user is seeking to gain access to “is typically unaware of the credential that was supplied by the user to the authentication system 210.” Ex. 1031, Col.7:57-60. Substitute claims 26 and 41 both require that “the server” running “the application” makes the determination of whether the first and second devices are in possession of the user based on the user being logged into the “application using application specific authentication information that is not authentication information specific to a device” and the authentication information is different for each device. *Gui* authentication system issues a “user profile and/or ticket” to the users device which is in turn provided to the service for authentication. In *Gui*, the server running the application (the “service”) does not know what type of authentication credentials were supplied to the authentication system. Similarly, applying *Gui* to *Takahashi*, the server would also not know whether the authentication information used to login to two separate devices was different because the authentication system does not convey this information to the service. Ex. 1031, Col.7:57-60.

221. *Gui*’s authentication system also undermines the security benefits of Substitute Claims 26 and 41 achieve by **requiring** two different passwords. Indeed, combining *Gui* with *Takahashi* reduces the security of *Takahashi*’s authentication

scheme because *Takahashi* already requires use of two different passwords where *Gui* does not. An attacker that gains access to the login information on the first device using *Gui*'s authentication system can use the same login information on the second device.

222. In my opinion, there is also no motivation to combine *Takahashi* with *Gui*. Petitioner suggests a POSITA would have been motivated to combine *Gui* with *Takahashi* to make authentication easier on different types of devices by allowing different authentication credentials. Pet. Opp. at 35. *Takahashi* already discloses a two password scheme where the mobile device automatically uses device specific "identification information" to authenticate to the second device which is an even easier authentication process than disclosed by *Gui* which still requires the user to input their authentication credentials. Compare Ex. 1007 ¶110 (*Takahashi*) with Ex. 1030, Col.2:20-47 (*Gui*). In sum, *Gui* discloses a less secure and less "user friendly" authentication system than the system already disclosed by *Takahashi*.

XII. ZHA, TAKAHASHI AND TSUSHIMA ARE NOT ANALOGOUS ART

223. Petitioner's Opposition to Dr. Rubin's Motion relies on several secondary references – *Kling*, *Lipetz*, *Gui* and *Lim*. All four references are instructive because they all address issues of security with online transactions

making them analogous prior art. In contrast, *Zha*, *Tsushima* and *Takahashi*, have nothing to do with security yet are put forth as “primary” obviousness references.

224. It is my understanding that the Parties generally agree that a POSITA at the time of invention of the '376 Patent would have had 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 security and/or network design and security. Notably, the Petitioner and Dr. Rubin agree a POSITA would have professional experience in the field of security.

225. The Board Preliminary Guidance defines the relevant “field of endeavor” as a “system or method in which as user interacts with a first [electronic] device and a second [electronic] device throughout the use of an online application.” PG at 18, 24-25. In my opinion, the Board has construed the field of endeavor for the '376 Patent well beyond reasonable scope of the '376 Patent.

226. First, the title of the patent is “Utilization of Multiple Devices To Secure Online Transactions.” Ex. 2005, p.1.

227. Second, the field of invention is defined as relating “generally to securing communications against malware by utilizing two devices with differential or application-specific components during an online session.” Ex. 2005, ¶2.

228. Third, the Abstract states that the “invention described herein can be configured for securing communications against malware by utilizing two devices with differential or application-specific components during an online session.” Ex. 1001, Abstract.

229. Fourth, the “Detailed Description” of the invention states in the very first paragraph that:

The present invention describes a system where the user has persistent use of a first device and a second device throughout the use of an online application to prevent a compromise of the transaction if malware infects either device.

Ex. 2005, ¶18.

230. Fifth, each disclosed embodiment in the '376 Patent relates to improving online security using two devices.

231. Sixth, each claim specifies it is directed to protecting information online. For example, the preamble of independent Substitute Claim 26 states “A method for *protecting information* by transmitting information to multiple electronic devices, the method comprising.” Similarly, Substitute Claim 26 provides that:

if and only if both the first and second devices are determined to be accessible by the server, then: transmitting the first subset of the information to the first device from the server; and transmitting the second subset of the information to the second device from the server, wherein the second subset of the information includes information not transmitted to the first device *thereby protecting the second subset of*

the information not transmitted to the first device from potential malware on the first device.

232. I have been informed by counsel that to “determine the applicable field of endeavor, the factfinder must consider ‘explanations of the invention's subject matter in the patent application, including the embodiments, function, and structure of the claimed invention.’” *Airbus S.A.S. v. Firepass Corp.*, 941 F.3d 1374, 1380 (Fed. Cir. 2019).

233. All of the claimed embodiments in Rubin are directed to securing an online session against malware using two devices with differential and/or application specific components. The title of the patent, the abstract, the background of the invention and the detailed description of the invention, all state the '376 Patent is to securing an online session against malware using two devices with differential and/or application specific components.

234. Additionally, all of the claims contain a preamble and claim limitation expressly directed towards protecting information from potential malware on a first device. Moreover, Substitute Claims 28, 29, 30 and 35 all require sensitive information only be sent to the second device. The function and structure of the claimed invention is plainly directed towards protecting online information from potential malware using two devices.

235. Based on the foregoing, it does seem plausible that field of endeavor for the '376 Patent can exclude any reference to security. Accordingly, I respectfully

disagree that the '376 Patent field of endeavor can be defined as a “system or method in which as user interacts with a first [electronic] device and a second [electronic] device throughout the use of an online application.” PG at 18, 24-25.

236. Once the field of endeavor for the '376 Patent is properly defined, it becomes clear that *Zha*, *Tsushima* and *Takahashi* are not analogous prior art.

A. *Zha* is not Analogous Prior Art.

237. *Zha* is directed towards “interface display” on multiple terminals. Nothing in *Zha* relates to the field of online security generally, or securing communications against malware more specifically using two devices. *Zha* attempts to solve a much different problem than '376 Patent. *Zha* does not seek to solve any security related issues. As discussed in my first declaration, *Zha* assigns different access permissions for applications with more than one functional interface so that each terminal only receives data specific to its assigned functional interface. Ex. 1004, 2:59-3:15. According to *Zha*, this helps to reduce (i) network traffic and (ii) switching by the user. *Id.* The '376 Patent seeks to improve on the prior art of “two-factor authentication” by disclosing a system and method where “the user has persistent use of a first device and a second device throughout the use of an online application to prevent a compromise of the transaction if malware infects either device.” Ex. 2003, ¶18. The two problems being solved for are completely unrelated.

B. *Tsushima* is Not Analogous Prior Art

238. *Tsushima* field of endeavor and description of related art has no relation to computer security. *Tsushima*'s "Summary of Invention" describes inventing a "content providing system, and a control method thereof, that realizes a content service in which it is possible to provide a wide range of operation input to a user."

Ex. 1010, ¶11. *Tsushima*'s "Summary of Invention" further describes two aspects of the present invention including the use of a first device for operational input, a server for receiving the operational input, updating the display based on the operational input, and transmitting the updated display to a second "display unit."

Ex. 1010, ¶¶ 12, 13.

239. Consistent with the above description of the Summary of Invention, *Tsushima* claims a "content providing system" and "control method for a content proving system" comprising a first device for operational input, a server for receiving and updating screen and transmitting to a second device for display. *See, e.g.,* Ex. 1010, Claim 1 and 8.

240. Similar to *Zha*, *Tsushima* field of endeavor has nothing to do with computer security. *Tsushima* is focused on improving upon the conventional techniques of experiencing streaming video data whether from network games or a "video distribution service." Nothing in *Tsushima* relates to the field of online security generally, or securing communications against malware more specifically.

241. *Tsushima* is also directed to a much different problem than '376 Patent. As discussed above, the '376 Patent is directed at responding to malware that may have compromised a user's device. The '376 Patent addresses this problem by using online applications designed to require two devices where chosen information is only disclosed to the second device in case the first device is compromised by malware. Ex. 2003, ¶¶3-7. *Tsushima*, on the other hand, seeks to provide a wider range of “operational inputs” for a user when using a mobile device as the controller for a video display (whether a game or a video) on a separate “display device.” Ex. 1010, ¶¶10-11. There is simply no relation to the problem addressed by *Tsushima* and the problem addressed by the '376 Patent.

242. Because *Tsushima* pertains to a different “field of endeavor” than the '376 Patent and attempts to solve a different problem than the '376 Patent, in my opinion *Tsushima* is not analogous prior art.

C. *Takahashi* is Not Analogous Prior Art.

243. In my opinion a POSITA would not consider *Takahashi* analogous prior art. As discussed above, the field of endeavor for the '376 Patent is online security. While the preferred embodiment is directed to “online games” the invention can be applied to any number of online activities “such as online banking, mobile healthcare, online investing, and other online activities that would benefit from enhanced security against malware on a user's computing device.” Ex 2003,

¶20. Accordingly, a POSITA would not look broadly to “online games”, “online banking”, “mobile healthcare”, “online investing” and “other online activities” for prior art relevant to the '376 Patent, unless the prior art was also directed to enhancing security. Otherwise, the scope of potentially relevant prior art would be unbounded.

244. *Takahashi* is directed to “a game control device” for online games. *Takahashi*'s field of endeavor relates to techniques “for controlling game progress with a communications terminal.” Ex. 1007, ¶2. Nothing in *Takahashi* relates to the field of online security generally, or securing communications against malware more specifically. Additionally, Dr. Rubin's invention is directed at securing online transactions within an application designed specifically to utilize two external devices. *Takahashi*'s “game control device” works with one device, or two devices. So even in the vast field of online games, *Takahashi* “game control device” is directed at online games using at least one external device, where all the online applications that could apply the teachings of the '376 Patent require two devices.

245. *Takahashi* attempts to solve a much different problem than '376 Patent. As discussed above, *Takahashi* is directed to a “game control device” that can be carried out on one device, or two devices. The '376 Patent attempts to secure online transactions by use of two devices. Because *Takahashi* attempts to solve a different

problem, and is in a different field of endeavor from the '376 Patent, it is my opinion *Takahashi* should not be considered analogous prior art.

XIII. CONCLUSION

246. I currently hold the opinions that I have expressed in this declaration. However, my analysis may continue, and I may acquire or receive additional information or insights that may result in revised or supplemental observations or opinions.