

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

FINTIV, INC.,

Patent Owner

Case No.: IPR2023-00399

U.S. Patent No. 9,208,488

Title: USING A MOBILE WALLET INFRASTRUCTURE TO SUPPORT
MULIPLE MOBILE WALLET PROVIDERS

**DECLARATION OF MICHAEL I. SHAMOS, PH.D.
IN SUPPORT OF PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MATERIALS CONSIDERED	2
III. SUMMARY OF MY OPINIONS	2
IV. LEGAL PRINCIPLES.....	3
V. LEVEL OF ORDINARY SKILL IN THE ART	3
VI. CLAIM CONSTRUCTION	5
A. “integration tier ... including web services communication mechanisms”	5
B. “web services communication mechanisms for interfacing with a mobile wallet application”	5
C. “different communication channels”	6
D. “mobile device”	6
E. “mobile wallet application”	7
F. “hardware SIM card”	8
VII. THE PETITION FAILS TO DEMONSTRATE THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE	13
A. Dill And Bykov Fail To Teach A Mobile Wallet Installed On A Hardware SIM Card.....	13
B. Dill Does Not Teach an Integration Tier That Includes a Web Services Communication Mechanism for Interfacing with a Mobile Wallet Application”	19
C. Dill Does Not Teach an Integration Tier That Includes Web Services Mechanisms for Interfacing with a Plurality of Different Device Types Over a Plurality of Different Channels	25
D. Petitioner Has Not Identified a Notification Services Engine Configured to Interface with the Integration Tier as Claimed	26
E. Dill Does Not Teach an Integration Tier That Includes Web Services Communication Mechanisms for Interfacing with a Plurality of Different Device Types Over a Plurality of Different Channels	27
F. The Petition Erroneously Maps Dill’s Mobile Wallet Application 121 in Mobile Network Operator 120 to the Claimed “Mobile Wallet Application” Installed on a Mobile Device	30
VIII. CONCLUSIONS	33

I. INTRODUCTION

1. My name is Michael Shamos. I have been retained as an expert witness by Patent Owner Fintiv, Inc. (“Fintiv” or “Patent Owner”) for this *Inter Partes* Review IPR2023-00399 of U.S. Patent No. 9,208,488 (the “’488 Patent” or the “Patent”) filed by Apple Inc. (“Apple” or “Petitioner”). I previously submitted a declaration in the matter entitled, “Declaration of Michael I. Shamos. Ph.D.,” dated April 11, 2023 (“Shamos I”).

2. In the Petition, I understand that Petitioner is challenging the validity of Claims 1-22 (the “Challenged Claims”) of the ’488 Patent (Ex. APPL-1001), constituting all the claims of Patent, on the grounds of obviousness. I have been asked to prepare the present declaration to be submitted with Patent Owner’s Response.

3. My background, qualifications and compensation were detailed in ¶¶ 5-17 of Shamos I.

4. This Declaration contains statements of my opinions formed in this case to date and the bases and reasons for those opinions. The statements made and opinions provided in this Declaration are based on my own personal knowledge. I may offer additional opinions based on further review of materials in this case, including opinions and/or testimony of other expert witnesses.

5. In this Declaration, all emphasis in boldface has been added unless otherwise noted.

II. MATERIALS CONSIDERED

6. I have reviewed the following documents in forming the opinions expressed in this Declaration I have considered all the materials cited herein and all materials filed in this IPR up to and including October 13, 2023.

7. I have also relied on my education, skill, training, and experience in the relevant fields of technology in forming my opinions. I have further considered the viewpoint of a person of ordinary skill in the art (“POSITA”) as of the time of the inventions of the ’488 Patent.

8. I reserve the right to supplement my opinions as expressed in this Declaration to address any new information obtained in the course of this proceeding, or based on any new positions taken by Petitioner.

III. SUMMARY OF MY OPINIONS

9. It is my understanding that the following table summarizes the grounds of challenge to the Challenged Claims raised in the Petition:

Ground	Invalidity Challenge	References	Challenged Claims
1	§ 103	Dill, Vadhri, and Akashika	1-22

10. After a review of the alleged prior art asserted by Petitioner and the Houh Declaration, it is my opinion that Petitioner has not demonstrated that the

claims are unpatentable on the sole ground of the Petition. My opinions, and the bases therefore, are detailed throughout this Declaration.

IV. LEGAL PRINCIPLES

11. The legal principles on which I was asked to rely were detailed in ¶¶ 25-32 of Shamos I.

V. LEVEL OF ORDINARY SKILL IN THE ART

12. I explained in ¶¶ 33-35 of Shamos I that a POSITA would have had “a bachelor’s degree in electrical engineering, computer science, or equivalent training, and approximately two years of work experience in software development with a working knowledge of mobile payment systems and techniques and a basic knowledge of accounting. Lack of work experience can be remedied by additional education, and vice versa.”

13. On p. 9 of the Institution Decision, the Board adopted this characterization: “a bachelor’s degree in electrical engineering, computer science, or equivalent training, and approximately two years of work experience in software development with a basic knowledge of accounting” and “working knowledge of mobile payment systems and techniques.” I believe that this characterization is substantially similar to mine, and I have adopted it for the purposes of this Declaration. I do not believe there to be any material differences between the two characterizations.

14. I have had at least this level of skill since at least 2010, when I regularly began teaching about mobile payment systems.

15. The opinions I express herein are from the viewpoint of such a POSITA as of November 21, 2011, the priority date assumed by Petitioner¹. Pet. at 3.

16. However, I think it is necessary to clarify what “a working knowledge of mobile payment systems and techniques” entails. Mere knowledge of payment systems generally, e.g., credit card clearing networks, would not be sufficient. “Mobile payments” are payments made from mobile wallets and the claims of the ’488 Patent specifically recite mobile wallets and mobile wallet applications.

17. Some payments can be made from mobile device without the use of a mobile wallet, such as when uses a mobile phone browser to buy an item from Amazon.com with a credit cards. These are not the type of mobile payments to which the ’488 Patent is directed. Therefore, a person who has a working knowledge of such online payment systems, but lacks a working knowledge of mobile wallets, would not be considered a POSITA in the field of the ’488 Patent.

¹ The Petition at 3 assumes a priority date of November 2011. The ’488 Patent claims priority to November 21, 2011.

VI. CLAIM CONSTRUCTION

18. Before delving into claim construction, I will explain the plain and ordinary meaning of certain claim terms as used in the '488 Patent.

A. **“integration tier ... including web services communication mechanisms”**

19. Each Challenged Claim recites an “integration tier ... including web services communication mechanisms for interfacing with” By the plain and ordinary meaning of “including,” this limitation requires that the web services communication mechanisms be included in (i.e., are part of) the integration tier, meaning that the integration tier provides the web services communication mechanisms. This is true for the simple reason that no other element of the Challenged Claims is recited as providing the web services communication mechanisms.

B. **“web services communication mechanisms for interfacing with a mobile wallet application”**

20. The limitation “web services communication mechanisms for interfacing with a mobile wallet application” plainly and literally require that the web services communication mechanisms must interface with a mobile wallet application. As I explain below in ¶ 27, the mobile wallet application resides on a mobile device, not some other platform that is not a mobile device. Therefore, the web services communication mechanisms must interface with a mobile wallet application that resides on a mobile device.

C. “different communication channels”

21. The “web services communication mechanism” are claims as being included in the “integration tier,” Therefore, the claim phrase “web services communication mechanisms for interfacing with ... a plurality of different device types over a plurality of different communication channels” plainly and literally means that the “different communication channels” must (1) interface with the “web services communication mechanisms”; and (2) connect the “integration tier” to the “different device types” outside of the “integration tier.” Plainly this also means that the “different communication channels” cannot be completely contained within “the integration tier.”

22. Clearly, then, a “communication channel that does not interface with “web service communication mechanisms” is not within the scope of the claimed “different communication channels.”

23. I understand that Patent Owner believes that three phrases, not including Petitioner’s phrase, actually require construction. I address Patent Owner’s phrases below.

D. “mobile device”

Claim Phrase	Patent Owner’s Construction
“mobile device” (Claims 1, 11 and 22)	“physical device that is mobile, such as a phone or tablet”

24. I agree with the Board’s adoption of this construction. Normally no construction of this well-understood term would be needed. However, Petitioner identified various structures in the prior art as “mobile devices” that are clearly not mobile devices. The Petition at 32 asserts that Sender’s M-Wallet 125 and Recipient’s M-Wallet 130 are “mobile devices” meeting limitation 1.4C. However, M-Wallets 125 and 130 are not devices at all – they are software and data residing not on a mobile device, but on the mobile network operator’s platform 130.

25. It appears that Petitioner is implicitly construing “mobile device” to include any element associated with a mobile network operator, whether or not that element is mobile. However, the Patent discloses at 11:14-15 that “[t]he subscriber has (or has access to) a mobile device 206 such as a phone or tablet.”

26. Possibly Petitioner has misconstrued the next sentence of the Patent (11:15-16), “[t]he mobile device runs the native or third party mobile wallet application 207.” In Dill, Mobile Wallet Application/Service 121, which includes M-Wallets 125 and 130, runs on the Mobile Network Operator platform 120. Petitioner apparently believes that any device that runs a mobile wallet application is a “mobile device,” which is incorrect.

E. “mobile wallet application”

Claim Phrase	Patent Owner’s Construction
--------------	-----------------------------

“mobile wallet application” (Claims 1, 11 and 22)	“wallet application installed on a SIM card or elsewhere on a mobile device”
---	---

27. This term is expressly defined in the Patent: “[a]s used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device.” Ex. 1001, 7:1-3.

28. Further, given that the claim language itself distinguishes between a “mobile device” and a “mobile wallet application,” a POSITA would have also understood that these terms have different meanings.

29. Petitioner points to Dill as using the term “mobile wallet application,” which it does. However, Petitioner points to “mobile wallet applications” in Dill that run on a mobile network operator’s platform. These are not “mobile wallet applications” as claimed in the Patent because they are not installed on a SIM card or elsewhere on a mobile device.

F. “hardware SIM card”

Claim Phrase	Patent Owner’s Construction
“hardware SIM card” (Claims 1, 11 and 22)	“secure, tamper-resistant chip on a mobile device that is separate from the mobile device’s main memory that enables the mobile device to access the cellular network”

30. A POSITA would have understood that “SIM” is the abbreviation for “Subscriber Identity Module,”² and that a SIM Card is “a smart chip that was designed as a secure, tamper-resistant environment.”³ The secure, tamper-resistant environment was originally designed in the 1990s for storing the cryptographic keys that GSM (Global System for Mobile Communications) carriers used to authenticate individual subscribers to the network connection and track those subscribers’ activities. However, by 2001, the SIM had evolved to have “about the same computing power as the first IBM PC.”⁴ As explained by one reference from the time, “[t]he SIM is the smaller of two computer chips inside a GSM mobile handset,” and a software developer would run their application on the SIM as compared to the main memory and processor of the mobile phone because “SIM-based applications are about taking action with the assurance that the data on which the action is based is from who it says it is from (authenticated and non-reputable), that it hasn’t been tampered with (integrity), and that nobody else is privy to what is happening (confidentiality).”⁵

² Guthery, Scott C.; Guthery, Scott C.; Guthery, Scott C.; Cronin, Mary J.; Cronin, Mary J.; Cronin, Mary J., *Mobile Application Development with SMS and the SIM Toolkit* (McGraw-Hill Telecom Professional) (p. 20). McGraw Hill LLC. Kindle Edition (2002) [Ex. 2021].

³ *Id.*, at 20 [Ex. 2021].

⁴ *Id.*, at 21-22 [Ex. 2021].

⁵ *Id.*, at 144 [Ex. 2021].

31. Yet, “[t]hroughout its evolution, the SIM has never lost sight of its primary function—to authenticate the subscriber to the network.”⁶ Specifically, the SIM card contains the International Mobile Subscriber Identity (IMSI)⁷ and a subscriber authentication key (Ki)⁸ used for authenticating the user on the network, ensuring that services are provided securely and effectively. Accordingly, when a mobile device attempts to connect to a GSM network, the IMSI is used during the authentication process. The network uses the IMSI to fetch the subscriber's details from the Home Location Register (HLR)⁹ or Visitor Location Register (VLR)¹⁰ and verify their credentials using an authentication algorithm and a Ki stored on the SIM. Once the authentication is successful, the subscriber is allowed access to the network services (e.g., voice calls, SMS

⁶ *Id.*, at 150 [Ex. 2021].

⁷ GSM 11.11 - Version 5.3.0 - Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; (GSM 11.11) (etsi.org) at Pg. 52 [Ex. 2022]

⁸ *Id.*, at 27.

⁹ Techopedia, "Home Location Register" definition (last updated November 17, 2011) (<https://www.techopedia.com/definition/7580/home-location-register-hlr>) [Ex. 2023]

¹⁰ Techopedia, "Visitor Location Register" definition (last updated September 12, 2011)(<https://www.techopedia.com/definition/9951/visitor-location-register-vlr>) [Ex. 2024]

messages, and data). Therefore, “[t]he SIM is like a key, without which the mobile phone can’t function.”¹¹

32. A POSITA’s understanding of a hardware SIM card as “a secure, tamper-resistant smart chip that is discrete from the mobile device’s main memory that enables the mobile device to access the cellular network” is further supported by the ’488 Patent specification, which states that the mobile wallet application may be installed on the device’s SIM card, or on the device’s main memory:

*As used herein, a mobile wallet application is a mobile wallet application installed on a SIM card or elsewhere on a mobile device.
Ex. 1001, 7:1-3 (emphasis added).*

* * *

The term “subscriber” refers to a participant of the mFS mobile wallet platform. The subscriber maintains a mobile wallet balance and performs transactions using the mFS application. An “unbanked subscriber” is a subscriber that does not have (or does not have access to) a bank account or credit union account. The application or “mobile wallet application” provides mobile wallet functionality to the (unbanked) subscriber. The mobile wallet application is installed on a mobile device in the device's memory, on a SIM card (such as a GSM SIM card) or is otherwise accessible to the mobile device. The

¹¹ The GSM Standard, An Overview Of Its Security, SANS Institute 2000-2002 (<https://www.giac.org/paper/gsec/1499/gsm-standard-an-overview-security/102787>) (giac.org), at 3 [Ex. 2025]

mobile wallet application provides the subscriber the ability to securely perform subscriber functions such as making retail purchases, paying bills, or transferring money to other mFS subscribers and non-subscribers. The mobile wallet application communicates with the mFS platform using binary and text SMS messages, among other forms of wireless communication. A wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates. Ex. 1001, 9:26-44 (emphasis added).

* * *

*It should also be noted that the mobile device **206** may be any type of plan-based phone or tablet, or prepaid phone or tablet. Many subscribers, such as unbanked subscribers, may primarily use prepaid phones. The mobile wallet application **207** may be installed on both plan-based phones and prepaid phones. The mobile wallet application may be installed on the device's SIM card, or on the device's main memory. Accordingly, the monetary transaction system **200** may be accessed and used via substantially any type of plan-based or prepaid mobile device. Ex. 1001, 12:7-16 (emphasis added).*

33. Accordingly, a POSITA would understand that a hardware SIM card is a secure, tamper-resistant smart card that is discrete from the mobile device's main memory that enables the mobile device to access the cellular network.

VII. THE PETITION FAILS TO DEMONSTRATE THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Dill And Bykov Fail To Teach A Mobile Wallet Installed On A Hardware SIM Card

34. In the Challenged Claims, “the mobile wallet application is installed on a hardware SIM card.” In the GSM embodiment set forth in the specification, “a wireless service provider or MNO provides the GSM network infrastructure on which the mFS platform operates,” and the mobile wallet application is installed on a “GSM SIM card.” (Ex. 1001, 9:33-34). A POSITA would have understood that a mobile subscriber must have a SIM installed on his or her device in order to access a GSM network. A POSITA would also have understood that Short Messaging Service (SMS) messages (which can also be referred to as text messages) are sent over the cellular network, and that for cellular networks like GSM that rely on SIMs, a mobile subscriber must have the SIM installed on his or her device in order to send and receive SMS messages.¹²

35. The Challenged Claims make clear that the mobile device (with the mobile wallet installed thereon) must have a functioning SIM, because the claims recite that the mobile device both sends and receives SMS/text messages. For example, claim 1 recites in part:

¹² As explained in Section IV(C), *supra*, a hardware SIM card is “secure, tamper-resistant chip on a mobile device that is separate from the mobile device’s main memory that enables the mobile device to access the cellular network.”

an integration tier configured to manage mobile wallet sessions with a mobile device and including web services communication mechanisms for interfacing with a mobile wallet application installed on a hardware SIM card as well as with a plurality of different device types over a plurality of different communication channels, the integration tier being configured to receive binary and text messages from the mobile device;

a notification services engine configured to interface with the integration tier and to send Short Message Peer-to-Peer (SSMP) messages, Short Messaging Service (SMS) messages and Simple Mail Transfer Protocol (SMTP) messages over the different communication channels to different devices, including the mobile device, to interface with the mobile wallet application installed on the hardware SIM card...

36. Thus, in the Challenged Claims, (i) the mobile wallet application must be installed on a hardware SIM card of the mobile device, and (ii) the mobile device must be operable to receive SMS messages over a cellular infrastructure. See, construction of “hardware SIM card” at (IV)(C)(a hardware SIM card, inter alia, “... enables the mobile device to access the cellular network.” A POSITA would have understood that these two requirements are interrelated, in that the SIM is required for the mobile device to gain access to the cellular network, and then, via access to mobile network, the mobile device is able to receive SMS messages over the cellular network.

37. The Petition makes two related arguments with respect to the hardware SIM card required by the Challenged Claims. In this regard, the Petition asserts:

Dill's mobile wallet application is installed on a hardware SIM card. APPL-1003, ¶95. Dill teaches "a mobile device communicatively coupled with the mobile communications network and executing a mobile wallet application." APPL-1005, claim 1. Dill's software instructions (including mobile wallet application) may be implemented on any type of "machine-readable mediums suitable for storing electronic instructions" which a POSITA would have understood to include a hardware SIM card. APPL-1005, [0106]; APPL-1003, ¶95. As evidenced by Bykov, SIM cards are commonly used to execute code for mobile transactions in mobile devices. APPL-1013, [0027]-[0028]; APPL-1003, ¶¶96-97. Thus, Dill teaches [1.3B]. APPL-1003, ¶¶97-98. (Pet., at 23-24).

These arguments are addressed below.

1. Dill Does Not Teach Installation Of A Mobile Wallet Application On A Hardware SIM Card

38. Dill never mentions a hardware SIM card. The terms "SIM" and "subscriber identification module" do not appear in Dill. The Petition asserts that Dill teaches installation of a mobile wallet application on a hardware SIM card, based on a boilerplate sentence at the end of Dill which includes a laundry list of potential storage mediums (none of which are SIM cards) and then ends with the

catch-all phrase “or other types of machine-readable mediums suitable for storing electronic instructions.” Ex. 1005, [0106]. The Petition latches on to this catch-all phrase, asserting that it teaches installing Dill's mobile wallet application on a hardware SIM card. A boilerplate, catch-all phrase such as “other types of machine readable mediums” is insufficiently specific to teach installation of the mobile wallet application on a hardware SIM card, as claimed. *See, Fromson v. Anitec Printing Plates, Inc.*, 132 F.3d 1437, 1447 (Fed. Cir. 1997) (“a boilerplate statement that other ‘suitable liquids’ can be used is insufficiently specific to include dissolving electrolytes such as are used by Fromson”); *Wasica Fin. GmbH v. Cont’l Auto. Sys.*, 853 F.3d 1272, 1285 (Fed. Cir. 2017) (“It is well established that disclosure of a genus in the prior art is not necessarily a disclosure of every species that is a member of that genus”); *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1367 (Fed. Cir. 2004)(“A prior art reference that discloses a genus still does not inherently disclose all species within that broad category.”)

2. Bykov and Dill Fail to Teach a Mobile Device in Which the Mobile Wallet Application is Installed on the Device’s Hardware SIM Card and the Mobile Device Can Access the Cellular Infrastructure, as Claimed

39. Bykov explains that “[o]ne of the challenges with mobile wallets ... is protection of the software code that handles sensitive information.” Ex. 1013,

[0002]. To meet this challenge, Bykov emphasizes the need to separate the software for the mobile wallet from all of the other software on the phone:

If the code runs on the same processor and in the same environment as other software components of the phone, it may be difficult or impossible to ensure isolation of the sensitive code and data as it can be compromised by other software running on the phone.

Ex. 1013, [0002].

40. As Bykov also explains, a related challenge for storage of wallet mobile solutions involves the reluctance of mobile network operators to provide financial institutions with access to the phone:

... some mobile wallet solutions may be blocked by the conflict of interests, ownership, and business models between mobile service providers and financial institutions. Both parties have their own relations with the customer: for the service providers, the customer is a mobile phone subscriber, for the financial institution, the same customer is an accountholder. The service providers may refuse to give access to the phone software by any external application considering it their asset. The financial institutions may be reluctant to have the service providers involved in their transactions and fees.

Ex. 1013, [0021]

41. Based on this background, Bykov teaches an embodiment in which a hardware card “in SIM form” is provided by a financial institution and can be

plugged into a SIM card slot in a cellular phone. Ex. 1013, [0026]-[0027]. This could be done either by (1) removing the SIM card provided by the cell provider and inserting the SIM form card of the financial institution; or (2) inserting the SIM form card in a second SIM card slot in the cellphone.

42. Bykov discloses that this “SIM form” card can be used to make a payment at a POS terminal using near-field communication (NFC). Ex. 1013, [0019], [0033], [0041], [0048]. Bykov does not disclose use of the “SIM form” financial institution card over a cellular network. It is important to understand that the “SIM form” financial institution card is NOT a “SIM card,” although it may be inserted into a SIM card slot for electrical purposes. It is not a “SIM card” because it does not identify the cellphone o a cellular network (or otherwise enable the cellphone to access the cellular network) – its only purpose is to make payments by NFC.

43. Given that the ”SIM form” card is being supplied by a financial institution, a POSITA would have understood that this card would not have included the credentials and functionality of a true SIM card, which are required to gain access the cellular network. Without access to the cellular network, a mobile device is unable to send and receive SMS messages, as required by the Challenged Claims.

44. As emphasized above, in the Challenged Claims the (i) mobile wallet application must be installed on a hardware SIM card of the mobile device, and (ii) the mobile device must be operable to receive SMS messages over a cellular infrastructure. Bykov does not teach that the financial institution card is a SIM card. In Bykov, if original SIM card is replaced by the financial institution card, the mobile device cannot send or receive SMS messages over the cellular network. If the financial institution card is inserted in a second SIM slot so that the original SIM card is still presented, then there is no “mobile wallet application installed on a hardware SIM card,” as claimed. In either case, Bykov does not teach the limitations requiring “a mobile wallet application installed on a hardware SIM card” or “interfac[ing] with the mobile wallet application installed on the hardware SIM card. For these reasons, the relied on references fail to meet all of the limitations of the Challenged Claims.

B. Dill Does Not Teach an Integration Tier That Includes a Web Services Communication Mechanism for Interfacing with a Mobile Wallet Application”

45. Dill does not teach a “web services communication mechanism” anywhere. A “web services communication mechanism” is not the same thing as a “web communication mechanism,” as Petitioner appears to believe. A “web service” is a term of art that refers to a service provided through a programming interface, such as an API. It is a computer-to-computer function invoked

automatically, and not at the request of user (like clicking on a hyperlink). There is no hint of web services in Dill.

46. “Web service” is a term of art that does not simply mean a “service offered over the Web. A “web service” communication involves a machine-to-machine interaction over the Internet using Web protocols. *See also*, e.g., *Web Services Architecture, W3C Working Group Note* (11 February 2004)(Ex. 2009, at 7)(“[a] Web service is a software system designed to support interoperable machine-to-machine interaction over a network”); Q. Mohmoud, *Service Oriented Architecture (SOA) And Web Services: The Road to Enterprise Application Integration (EAI)*(2005) (Ex. 2010) (“[w]eb services are software systems designed to support interoperable machine-to-machine interaction over a network”); R. Studer et al., *Semantic Web Services, Concepts, Technologies and Applications* (2007) (Ex. 2011) (“[a] web service is a software system designed to support machine-to-machine interaction over the internet”); *Electronic Services: Concepts, Methodologies, Tools and Applications* (2010) (Ex. 2012) (“[o]ne aim of introducing Web Services is to achieve machine-to-machine communication”); E. van de Kar et al., *Designing Mobile Service Systems* (2008) (Ex. 2013) (“[w]eb services provide machine-to-machine communication to enable interoperability between (distributed) applications”); I. Taylor et al., *From P2P And Grids To Services On The Web, Second Edition* (2009) (Ex. 2014)(“[w]eb services are a

software system designed to support interoperable machine-to-machine interaction over a network”); and C. Petrie et al., *Semantic Web And Beyond: Computing For Human Experience, Semantic Web Services Challenge, Results From The First Year* (2009) (Ex. 2015) (“[w]eb services are software systems designed to support interoperable machine-to-machine interactions over a network.”) Dill does not disclose any “web services,” hence does not disclose any “web services communication mechanism.”

47. “Web services communication mechanisms” are claimed as “interfacing with a mobile wallet application” on a mobile device, which makes clear that the “web services” are in fact machine-to-machine communications (i.e., between the mobile wallet application on a mobile device and the integration tier).

48. The Petition maps the claimed “web services communication mechanisms” to Dill's web interface 137, which Dill simply describes as accessing a web site. For example, Dill [0033] refers to “a web site of the money transfer facilitator” and discloses that the sender may provide the money transfer facilitator with transaction information via a “web page”); [0034] (“web page notification”); [0035], [00051], [0054] (“a web site”); [0071], [0072], [0104] (“a website”). Providing a web site is not providing a “web service.” In its analysis, the Petition reads the word “services” completely out of the claim by erroneously

equating “web services communications mechanism” with “web communication mechanisms.”

49. Furthermore, Petitioner maps the “integration tier” to Dill's Transfer Options Module 145, and the claimed “web services communication mechanism” to Dill's web interface 137. Pet., at 23-24. The Petition does not identify any integration tier that includes web services communication mechanisms, as required by all of the Challenged Claims. The web services communication mechanisms for interfacing with the mobile wallet application must be included *within* the integration tier. Contrary the express claim language, Petitioner’s supposed “web services communication mechanisms” are Dill's web interface 137, which is *outside* of Dill's transfer options module 145 (which Petitioner maps to the “integration tier”).

50. This discrepancy is apparent from an annotated diagram of Petitioner’s mappings:

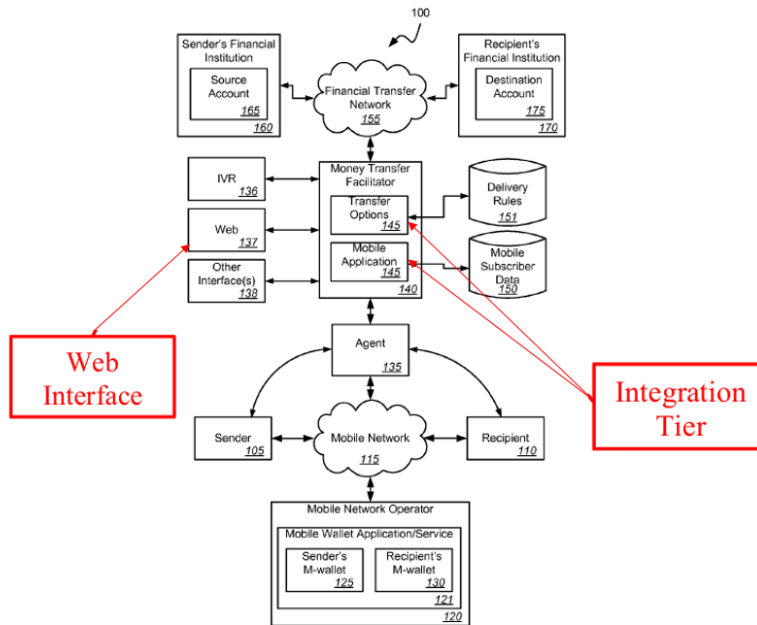


FIG. 9

51. Web Interface 137 is clearly outside what Petitioner maps to the “integration tier,” and Petitioner does not even attempt to show that any “web services communication mechanisms can be found anywhere in Transfer Options Module 145. Further detail of Petition’s mapping is shown in this annotated diagram:

Mapped to “web services communication mechanisms” that the claim requires to be included in the “integration tier”

Mapped to a communication channel *over which* the web services mechanisms (that the claim requires to be included in the “integration tier”) communicates with a different device type.

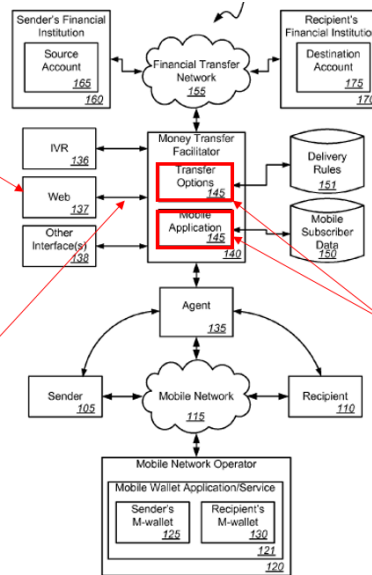


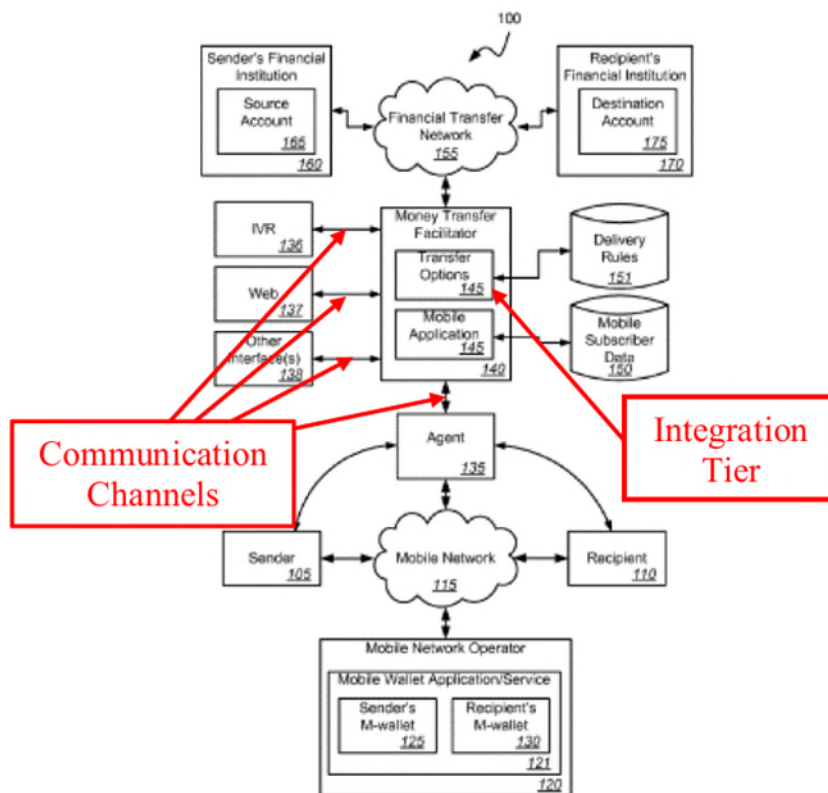
FIG. 9

52. A POSITA would have understood that the “different communication channels” with which the “web services communication mechanisms” communicate with different device types extend from the integration tier to those different device type (e.g., iPhone, Android phone or Blackberry as shown in Figure 1). If Dill’s web interface 137 (the supposed “web services communication mechanisms”) were somehow within Dill’s Transfer Option Module 145 (the supposed “integration tier”), then the connection from Dill’s web interface 137 that the Petition mapped to the “different communication channel” would be completely contained in the supposed integration tier, rather than extending from the integration tier to different device types, as claimed. This mapping is contrary to the plain meaning of the claims, in which the “different

communication channels” extend from the integration tier to different device types rather than being completely contained within the claimed integration tier.

C. Dill Does Not Teach an Integration Tier That Includes Web Services Mechanisms for Interfacing with a Plurality of Different Device Types Over a Plurality of Different Channels

53. In each Challenged Claim, the “web services communication mechanisms” included in the “integration tier” must interface with “a plurality of different device types over a plurality of different communication channels.” The annotated figure below shows how Petitioner mapped “communication channels” and “integration tier” to Dill:



54. In the above mapping, the claimed “communication channels” are apparently mapped to Dill IVR 136, Web 137, Other Interface(s) 138, and the unnumbered link between Agent 135 and Money Transfer Facilitator 140. None of those, however, is a “web services communication mechanism,” including “Web 137.” IVR 136 is a phone system and does not involve the Web at all. See Dill, [0092]. There is no teaching or suggestion in Dill that Other Interface(s) 138 have anything to do with the Web. Regarding Agent 135, Dill merely discloses that “[t]he system can also include an agent 135 in communication with the money transfer facilitator 140.” Dill, [0051]. There is no disclosure that this communication involves the Web in any way.

55. That leaves Web 137, which surely is a web interface. However, as explained above, Dill does not teach any “web services,” hence no “web services communication mechanism.” Even assuming (erroneously), that a web service is offered over channel Web 137, one such channel does not constitute the claimed “plurality of different communication channels.”

D. Petitioner Has Not Identified a Notification Services Engine Configured to Interface with the Integration Tier as Claimed

56. Each Challenged Claim recites “a notification services engine configured to interface with the integration tier.” However, Petition maps the claimed “notification services engine” to the same element in Dill to which Petitioner mapped to the integration tier, namely, Dill’s Transfer Options Module

145. Pet., at 27. This creates the nonsensical situation in which the Integration Tier must interface with itself.

E. Dill Does Not Teach an Integration Tier That Includes Web Services Communication Mechanisms for Interfacing with a Plurality of Different Device Types Over a Plurality of Different Channels

57. In the claims, the “web services communication mechanisms” must “interface with a mobile wallet application.” As explained above, in the ’488 Patent, the mobile wallet application is installed on the mobile device. As further explained above, Dill does not teach any “web services” or “web services communications mechanism.” The Petition maps “web services communications mechanism” erroneously to Web interface 137 – erroneous at least because there is no disclosure that any web services are offered over that interface. Even assuming (erroneously) that a web service is offered over interface Web 137, there is no teaching in Dill that Web 137 interfaces with a mobile wallet application on a mobile device.

58. Dill discloses that, in an alternative embodiment, the mobile device may run a “mobile wallet application,” as that term is used in Dill, which, as explained above, is different from the claimed “mobile wallet application.” But, even assuming (erroneously) that both “mobile wallet applications” are the same, Dill does not teach that any communication with the ostensible “mobile wallet application” takes place over interface Web 137. On the contrary, in Dill, all

communications from a mobile wallet application on the customer's mobile device are routed first through mobile network 115, and are not described as passing through web interface 137:

As noted above, embodiments of the present invention provide methods and systems for supporting money transfer transactions initiated by and/or conducted through a variety of channels but are not limited to a wireless communication channel or systems including or using a wireless communication device. Therefore, according to still another embodiment, a money transfer facilitator system can comprise one or more interfaces for conducting money transfer transactions and a transfer options module communicatively coupled with the one or more interfaces. For example, the one or more interfaces can comprise at least one of an Interactive Voice Response (IVR) interface, a web interface, an interface to an agent system, or other interface. The transfer options module can be adapted to receive transaction information for a money transfer transaction from a sender through at least one of the interfaces, provide a notification of the transaction to a recipient of the transaction, and select one or more delivery options for completing the money transfer transaction.

Dill, [0047]

59. The above passage teaches that, when a sender initiates a transaction using the mobile wallet application executing on the sender's mobile device, the flow of that transaction is as shown in Figure 9 of Dill (through the MNO and agent to 140, rather than through web interface 137), and that Dill's web interface

137 represents an alternative way for a sender to initiate a transaction that does not use the mobile wallet application on the sender's mobile device. A similar teaching appears in Dill [0100]-[0101].

60. Therefore, a POSITA would not expect Dill's IVR 136 or Other Interface(s) 138 to interface with a mobile wallet application on a mobile phone (which would be nonsensical for a voice connection like IVR). Similarly, there is teaching in Dill that Web 137 communicates with a mobile wallet application on a mobile phone.

61. In [0104], Dill again distinguishes between wireless communication channels/wireless devices in some embodiments, against other embodiments involving the IVR, web interface, and other interface(s). Dill references "logging into a website" in connection with interfaces 136-138:

Such services can be provided to the recipient 110 in a variety of ways. For example, a notification can be provided to the recipient 110 via a mobile device and mobile network 115 as described above. Additionally or alternatively, a telephone call, telegram, email, SMS, U.S. postal letter, or other type of message can be sent to the recipient 110 providing the recipient 110 with notification of the transfer transaction and possibly instructions and/or options. Via one of the interfaces 136-138, e.g., by logging onto a website, calling an IVR, visiting an agent location, etc. depending upon the notification and/or instructions provided, the

recipient can select a delivery option and/or provide instructions for the delivery.

Dill, [0104]

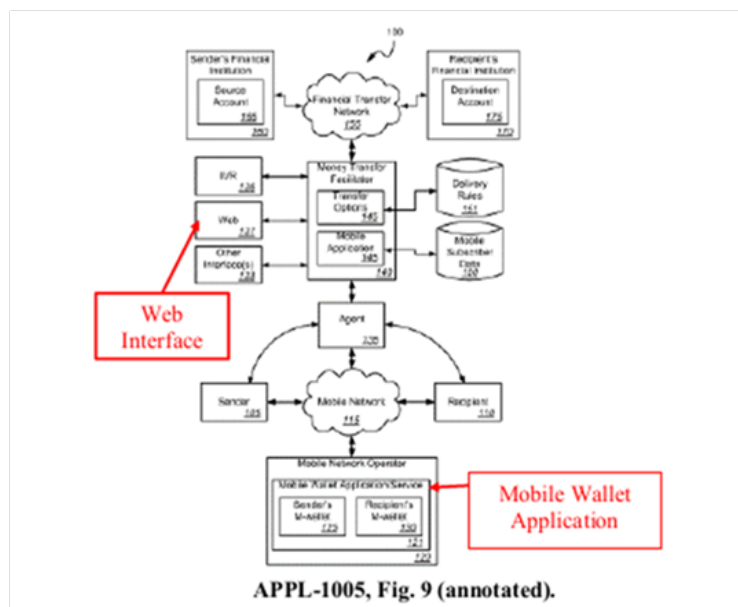
62. Even to the extent Dill teaches that a user “logs into a website” via interface 137, there is no basis for assuming that such a website log-in makes use of a mobile wallet application on a mobile phone. Further, Petitioner does not show, or even allege, that it is inherent in Dill that for Web 137 to communicate with a mobile wallet application on a mobile phone, as claimed. For example, if sender 105 used a browser on her mobile phone to log-in via Web 137, that would fail to meet the claim language because a browser is not a mobile wallet application installed on a mobile phone. The ’488 Patent further requires that the mobile wallet application be provided by either the provider of the cloud-based platform or a third party provider. EX1001, 7:3-7. A web page that a user simply views from a web site with his or her browser is not an application, as claimed.

F. The Petition Erroneously Maps Dill’s Mobile Wallet Application 121 in Mobile Network Operator 120 to the Claimed “Mobile Wallet Application” Installed on a Mobile Device

63. Dill’s teaching that a user “logs into a website” via interface 137, provides no basis for assuming that such a website log-in makes use of a mobile wallet application on a mobile device. Petitioner has not shown or even alleged that it is inherent in Dill that Dill’s Web 137 connects with a mobile wallet

application on a mobile phone, as claimed. For this further reason, the Petition has failed to carry its burden of demonstrating that the relied on references meet all of the limitations of the Challenged Claims.

64. The Petition does not even map the claimed “mobile wallet application” to an application installed on a mobile device. Rather, at page 23 of the Petition (shown below), the Petition maps the claimed “mobile wallet application” to Mobile Wallet Application/Service 121 located within Mobile Network Operator 120:



65. A POSITA would understand that Mobile Wallet Application/Service 121 in Dill’s Mobile Network Operator 120 is not installed on a mobile device, as required by all Challenged Claims of the ’196 Patent. The MNO platform that provides communication to cellphones is not itself a “mobile device” per the construction of that term.

66. There is no disclosure in Dill that the mobile wallet application, when running on the mobile device, performs anything other than the pull transaction described in [0094] and claimed in claim 13. For example, Dill explains that “the mobile wallet application 121 maintains mobile wallets 125 and 130 for one or more subscribers, such as the sender 105 and/or recipient 110 to the mobile wallet service 121.”

67. Dill does not explain how these M-wallets would be stored on the recipient’s device 110. Storing the sender’s M-wallet 125 on the recipient’s device 110 would represent a major security vulnerability and would be nonsensical to a POSITA. Mr. B is not entitled to hold Mr. A’s wallet on his own device. Instead, Dill refers “the mobile wallet application 121 of a mobile network operator 120” (Dill, [0054]) (“the mobile wallet application 121 of the recipient’s 120 wireless network operator 120”) (Dill, [0084], describing the functionality of the mobile wallet 121).

68. Accordingly, a POSITA would understand [0094] to include a typographical error because it would not make sense for the mobile wallet 121 that is described throughout Dill as running on the Mobile Network Operator 120 to run on the recipient’s device 110. Per Dill claim 13, [0094] describes a different Mobile Wallet Application that is “adapted to receive a Personal Identification

Number (PIN) and a transaction identifier for a previously initiated money transfer transaction.”

VIII. CONCLUSIONS

69. Relying on my education, experience, skill, and training in the relevant field of art, and after reviewing the materials identified above, it is my opinion that:

- Patent Owner’s proposed constructions correspond to the plain and ordinary meanings of the terms construed.
- Petitioner has not demonstrated a reasonable likelihood of success on its sole ground for the Petition.

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

71. I reserve the right to supplement my opinions in the future to respond to any arguments that Petitioner raises and to take into account new information as it becomes available to me.

72. In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal

Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination remotely within the United States during the time allotted for cross examination.

Executed October 13, 2023 at Pittsburgh, Pennsylvania.


Michael I. Shamos, Ph.D.