

2019-1628

**United States Court of Appeals
for the Federal Circuit**

BYTEMARK, INC.,

Plaintiff-Appellant,

— v. —

MASABI LTD.,

Defendant-Appellee.

*On Appeal from the United States District Court for the
Eastern District of Texas in Case No. 2:16-cv-00543-JRG-RSP*

BRIEF FOR PLAINTIFF-APPELLANT

DARIUSH KEYHANI
KEYHANI LLC
1050 30th Street, NW
Washington, DC 20007
(202) 748-8950
dkeyhani@keyhanillc.com

Counsel for Plaintiff-Appellant

MAY 6, 2019

FORM 9. Certificate of Interest

Form 9
Rev. 10/17

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

Bytemark, Inc. v. Masabi Ltd.Case No. 19-1628

CERTIFICATE OF INTEREST

Counsel for the:

☐ (petitioner) ☒ (appellant) ☐ (respondent) ☐ (appellee) ☐ (amicus) ☐ (name of party)

certifies the following (use "None" if applicable; use extra sheets if necessary):

1. Full Name of Party Represented by me	2. Name of Real Party in interest (Please only include any real party in interest NOT identified in Question 3) represented by me is:	3. Parent corporations and publicly held companies that own 10% or more of stock in the party
Bytemark, Inc.	Bytemark, Inc.	INIT Innovations in Transportation, Inc.
		HaCon Ingenieurgesellschaft mbH

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court (and who have not or will not enter an appearance in this case) are:

Dariush Keyhani
 Jennifer Meredith
 Frances Stephenson
 Meredith & Keyhani, PLLC
 Keyhani LLC
 Andy Tindel
 G. Blake Thompson
 MT2 Law Group

FORM 9. Certificate of Interest

Form 9
Rev. 10/17

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal. *See Fed. Cir. R. 47.4(a)(5) and 47.5(b).* (The parties should attach continuation pages as necessary).

Bytemark, Inc. v. Masabi Ltd., No. 2:16-cv-00543-JRG-RSP (E.D. Tex.)

Bytemark, Inc. v. Masabi Ltd., No. 19-1442 (Fed. Cir.)

IPR2017-01449 (USPTO)

Bytemark, Inc. v. Xerox Corp. et al., No. 1:17-cv-01803-PGG (S.D.N.Y.)

Bytemark, Inc. v. Token Transit, Inc., No. 1:18-cv-00834-MN-CJB (D. Del.)

3/19/2019

Date

/s/ Dariush Keyhani

Signature of counsel

Please Note: All questions must be answered

Dariush Keyhani

Printed name of counsel

cc: _____

Reset Fields

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	v
STATEMENT OF RELATED CASES	1
JURISDICTIONAL STATEMENT	2
STATEMENT OF ISSUES	3
STATEMENT OF THE CASE.....	4
STATEMENT OF FACTS	6
A. The Patents-in-Suit	6
1. The ‘967 Patent	6
2. The ‘993 Patent	8
B. Litigation of the Patents-in-suit.....	11
1. Litigation in the Eastern District of Texas.....	11
2. Litigation in other venues	13
3. Proceedings before the PTAB.....	15
SUMMARY OF ARGUMENT	16
STANDARD OF REVIEW	19
ARGUMENT	21
A. The District Court’s Grant of Summary Judgment Was Error Because There Is a Genuine Issue of Material Fact As to Whether The Claimed Inventions Are Patent-Eligible Subject Matter	21
1. Whether a claim element or combination of elements is well-understood, routine and conventional is a question of fact that must be proven by clear and convincing evidence	21
2. A reasonable jury could find that the claim elements of the patents-in-suit are not well-understood, routine, and conventional	24

3.	In determining that summary judgment was proper, the district court impermissibly relied on argument and issues outside of the parties’ briefing	29
4.	The pending office actions are not final determinations and, in fact, support the validity of the patents-in-suit	31
5.	The Court Erred by Not Limiting Masabi’s Arguments to Claim 1 of the ‘967 Patent and Claim 1 of the ‘993 Patent.....	33
B.	Even if There Is No Genuine Issue of Material Fact, the Patent Claims Are Subject-Matter Eligible Under § 101 As a Matter of Law	36
1.	The district court erroneously concluded that the claimed inventions of the ‘967 and ‘993 patents are directed towards an abstract idea	37
a.	The claims of the ‘967 and ‘993 patents improve a technological process	39
b.	The district court erred by focusing on claim elements in isolation and oversimplifying the claimed inventions	42
2.	The district court erroneously concluded that the asserted claims of the ‘967 and ‘993 patents lack an inventive concept	47
CONCLUSION		53

TABLE OF AUTHORITIES

	Page(s)
Cases:	
<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 890 F.3d 1354 (Fed. Cir. 2018)	21, 22
<i>Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.</i> , 728 F.3d 1336 (Fed. Cir. 2013)	53
<i>Alice Corp. v. CLS Bank Int’l</i> , 573 U.S. 208, 134 S. Ct. 2347 (2014)	passim
<i>Amdocs (Israel) Ltd. v. Openet Telecom, Inc.</i> , 761 F.3d 1329 (Fed. Cir. 2014)	19
<i>Amdocs (Israel) Ltd. v. Openet Telecom, Inc.</i> , 841 F.3d 1288 (Fed. Cir. 2016)	47
<i>Ancora Techs., Inc. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018), <i>as amended</i> (Nov. 20, 2018)	passim
<i>Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)	passim
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)	passim
<i>Bilski v. Kappos</i> , 561 U.S. 593 (2010).....	36
<i>Bytemark v. Xerox et al.</i> , 1:17-cv-01803-PGG, Dkt. No. 49 (S.D.N.Y.).....	1, 14, 28
<i>Bytemark, Inc. v. Masabi Ltd.</i> , 19-1442 (Fed. Cir.)	1, 15, 16
<i>Bytemark, Inc. v. Masabi Ltd.</i> , Civ. No. 2:16-cv-00543 (E.D. Tex.).....	1, 4, 11
<i>Bytemark, Inc. v. Token Transit</i> , Civ. No. 1:18-cv-00834 (D. Del.).....	1, 14
<i>Cap Exp., LLC v. Zinus, Inc.</i> , 722 F. App’x 1004 (Fed. Cir. 2018).....	19, 23

<i>ChargePoint, Inc. v. SemaConnect, Inc.</i> , 920 F.3d 759 (Fed. Cir. 2019)	34
<i>Cleveland Clinic Found. v. True Health Diagnostics LLC</i> , 859 F.3d 1352 (Fed. Cir. 2017), <i>cert. denied</i> , 138 S. Ct. 2621 (2018)	34
<i>Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.</i> , 776 F.3d 1343 (Fed. Cir. 2014)	33, 35, 53
<i>Core Wireless Licensing S.A.R.L. v. LG Electronics, Inc.</i> , 880 F.3d 1356 (Fed. Cir. 2018)	38
<i>Data Engine Techs. LLC v. Google LLC</i> , 906 F.3d 999 (Fed. Cir. 2018)	38, 43
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	37
<i>Diamond v. Diehr</i> , 450 U.S. 175 (1981).....	37
<i>E.I. du Pont De Nemours & Co. v. Unifrax I LLC</i> , No. 2017-2575, 2019 WL 1646491 (Fed. Cir. Apr. 17, 2019)	52
<i>Elec. Power Grp., LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016)	19-20
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016)	38, 39, 47
<i>Exergen v. KAZ USA Inc.</i> , 725 Fed. App'x 959 (Fed. Cir. 2018)	21, 24
<i>Finjan, Inc. v. Juniper Network, Inc.</i> , No. C 17-05659 WHA, 2018 WL 4184338 (N.D. Cal. Aug. 31, 2018)	25
<i>Greenlaw v. United States</i> , 554 U.S. 237 (2008).....	30
<i>In re Etter</i> , 756 F.2d 852 (Fed. Cir. 1985)	22, 23
<i>In re Morinville</i> , No. 2018-1895, 2019 WL 1890529 (Fed. Cir. Apr. 29, 2019)	24

<i>Intellectual Ventures I LLC v. Capital One Bank (USA),</i> 792 F.3d 1363 (Fed. Cir. 2015)	43, 44, 53
<i>Interconnect Planning Corp. v. Feil,</i> 774 F.2d 1132 (Fed. Cir. 1985)	22, 23
<i>King Pharms., Inc. v. Eon Labs, Inc.,</i> 616 F.3d 1267 (Fed. Cir. 2010)	37
<i>Lexion Med., LLC v. Northgate Techs., Inc.,</i> 641 F.3d 1352 (Fed. Cir. 2011)	19
<i>Massey v. Del Labs., Inc.,</i> 118 F.3d 1568 (Fed. Cir. 1997)	19
<i>Maxwell, Ltd. v. ZTE (USA) Inc.,</i> 5:16-cv-00179-RWS, Dkt. No. 228 (E.D. Tex. June 29, 2018)	25
<i>Mayo Collaborative Servs. v. Prometheus Labs., Inc.,</i> 556 U.S. 66 (2012)	17, 20, 24, 37
<i>McRO, Inc. v. Bandai Namco Games Am., Inc.,</i> 837 F.3d 1299 (Fed. Cir. 2016)	36
<i>Mikkilineni v. Stoll,</i> 410 F. App'x 311 (Fed. Cir. 2010)	32
<i>Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.,</i> 811 F.3d 1314 (Fed. Cir. 2016)	20
<i>Openwave Sys. Inc. v. Apple Inc.,</i> 808 F.3d 509 (Fed. Cir. 2015)	38
<i>Perdiemco, LLC v. Industrack LLC,</i> No. 2:15-CV-1216-JRG-RSP, 2016 WL 5719697 (E.D. Tex. Sept. 21, 2016), <i>report and recommendation adopted</i> , No. 2:15-CV-727- JRG, 2016 WL 5475707 (E.D. Tex. Sept. 29, 2016)	33
<i>Pfizer, Inc. v. Apotex, Inc.,</i> 480 F.3d 1348 (Fed. Cir. 2007)	23
<i>Roche Molecular Sys., Inc. v. CEPHEID,</i> 905 F.3d 1363 (Fed. Cir. 2018)	19
<i>Smart Sys. Innovations, LLC v. Chi. Transit Auth.,</i> 873 F.3d 1364 (Fed. Cir. 2017)	43, 44, 45

<i>Smith v. Reg'l Transit Auth.</i> , 827 F.3d 412 (5th Cir. 2016)	19
<i>SRI Int'l, Inc. v. Cisco Sys., Inc.</i> , 918 F.3d 1368 (Fed. Cir. 2019)	36
<i>Thales Visionix Inc. v. United States</i> , 850 F.3d 1343 (Fed. Cir. 2017)	46
<i>Trading Techs. Int'l, Inc. v. CQC, Inc.</i> , 675 Fed. App'x 1001 (Fed. Cir. 2017)	37-38
<i>Ultramercial, Inc. v. Hulu, LLC</i> , 772 F.3d 709 (Fed. Cir. 2014)	52
<i>Uniloc USA, Inc. v. AVG Techs. USA, Inc.</i> , No. 2:16-CV-00393-RWS, 2017 WL 1154927 (E.D. Tex. Mar. 28, 2017)	33
<i>Uniloc USA, Inc. v. Samsung Elecs. Am., Inc.</i> , No. 2:17-CV-00651-JRG, 2018 WL 4927279 (E.D. Tex. Sept. 18, 2018)	25
<i>United States v. Green</i> , 508 F.3d 195 (5th Cir. 2007)	30
<i>Univ. Secure Registry, LLC v. Apple Inc.</i> , No. CV 17-585-CFC-SRF, 2018 WL 4502062 (D. Del. Sept. 19, 2018)	32
<i>Versata Software, Inc. v. NetBrain Techs., Inc.</i> , No. 13-676-LPS-CJB, 2015 WL 5768938 (D. Del. Sept. 30, 2015)	33-34
<i>Visual Memory LLC v. NVIDIA Corp.</i> , 867 F.3d 1253 (Fed. Cir. 2017)	38

Statutes & Other Authorities:

28 U.S.C. § 1295(a)(1)	2
28 U.S.C. § 1331	2
28 U.S.C. § 1338(a)	2
28 U.S.C. § 2107(a)	2

35 U.S.C. § 101	<i>passim</i>
37 C.F.R. §§ 1.111-1.112.....	32
Fed. R. App. P. 4.....	2
Fed. R. Civ. P. 56(a).....	19

STATEMENT OF RELATED CASES

No appeal in or from the present district court case has previously been before this Court or any other appellate court. The following cases pending in this Court and other courts will directly affect the Court's decision here:

Bytemark, Inc., v. Masabi Ltd., 19-1442 (Fed. Cir.)

The following cases may be directly affected by this Court's decision here:

Bytemark, Inc., v. Masabi Ltd., Civ. No. 2:16-cv-00543 (E.D. Tex.).

Bytemark, Inc. v. Xerox Corp. et al., Civ. No. 1:17-cv-01803 (S.D.N.Y.). The patent claims in this case have been dismissed without prejudice by stipulation of the parties.

Bytemark, Inc. v. Token Transit, Civ. No. 1:18-cv-00834 (D. Del.). This case has been stayed by the district court.

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 28 U.S.C. §§ 1331 & 1338(a) and entered a final judgment on February 7, 2019. This appeal, noticed on March 6, 2019, is timely. 28 U.S.C. § 2107(a); Fed. R. App. P. 4. This Court has jurisdiction under 28 U.S.C. § 1295(a)(1).

STATEMENT OF ISSUES

1. Whether the district court's grant of summary judgment of invalidity was error because there exists a genuine issue of material fact as to whether the claimed inventions are patent-eligible subject matter, and where

- (a) the district court failed to apply the controlling law;
- (b) Masabi failed to meet its summary judgment burden;
- (c) the district court relied on arguments and issues that were outside the parties' briefing; and

- (d) the district court failed to limit Masabi's arguments to claim 1 of the '967 patent and claim 1 of the '993 patent.

2. Whether the district court's grant of summary judgment of invalidity was error because the patent claims are subject-matter eligible under § 101 as a matter of law.

STATEMENT OF THE CASE

This is an appeal brought by patent owner Bytemark, Inc. (“Bytemark”) from a final judgment entered by the Eastern District of Texas on February 7, 2019, granting Masabi Ltd. (“Masabi”)’s motion for summary judgment of invalidity. (Appx1.) At issue in this appeal are two software patents: U.S. Patent No. 8,494,967 (“the ‘967 patent”) and U.S. Patent No. 9,239,993 (“the ‘993 patent”) (collectively, “the patents-in-suit”). The patents-in-suit, which share the same specification, are currently being litigated in multiple jurisdictions and have survived various post-grant proceedings before the Patent Trial and Appeal Board. The ‘993 patent, which issued after the U.S. Supreme Court’s decision in *Alice Corp. v. CLS Bank Int’l*, 134 S. Ct. 2347 (2014), was previously reviewed and approved by a USPTO § 101 expert post-*Alice*. (Appx3406.) Bytemark has invested considerable time, resources, and money into defending the patents-in-suit.

On May 20, 2016, Bytemark sued Masabi Ltd. (“Masabi”) in the United States District Court for the Eastern District of Texas for willful infringement of the patents-in-suit. *See Bytemark, Inc., v. Masabi Ltd.*, Civ. No. 2:16-cv-00543 (E.D. Tex.). On October 4, 2017, Masabi made its first challenge to the patents’ validity, filing a motion for summary judgment for invalidity (“Motion”). (Appx3193-3241.) In its Motion, Masabi, *inter alia*, argued that conflicting positions of the parties’ experts did not raise a genuine issue of material fact and incorrectly placed the

burden on Bytemark to “rebut” Masabi’s expert testimony or otherwise “concede[] to patent-ineligible subject matter.” (Appx3193-3241, Appx3213.) Masabi’s arguments were directed only towards claim 1 of each patent. (Appx3193-3241.) On October 20, 2017, Bytemark filed its opposition brief (“Opposition”), addressing the arguments that Masabi had made in its Motion. (Appx3244-3283.) Four days later, and before Masabi filed a reply brief, the district court removed the case from the trial docket without explanation. (Appx3448.) On February 14, 2018, the district court *sua sponte* stayed the case. (Appx3452.)

On November 26, 2018, more than one year after Masabi filed its Motion, and with no further summary judgment briefing having taken place, the magistrate judge issued a Report and Recommendation (“R&R”) recommending that Masabi’s Motion be granted and that the patents-in-suit be invalidated. (Appx3457-3474.) On February 7, 2019, the district court summarily adopted the R&R, determining that no reasonable jury could find the claims of the patents patent-eligible. (Appx1.) In its decision, the district court did not address the summary judgment standard, the parties’ burdens, or the factual evidence put forth by the parties. (Appx 1, Appx3457-3474.) The opinion, which issued in 2019, did not cite any cases decided after 2017. (Appx 1, Appx3457-3474.)

On March 6, 2019, Bytemark filed a notice of appeal to this Court.

STATEMENT OF FACTS

A. The Patents-in-Suit

Bytemark is the owner of all rights, title and interest in and to the ‘967 and ‘993 patents, which disclose and claim Bytemark’s V3 Ticketing Technology. (Appx85-111, Appx112-138.) Bytemark offers for sale visual validation mobile ticketing applications and systems disclosed and claimed by the patents-in-suit, including but not limited to, the V3 Ticketing Technology that is the subject of Bytemark’s infringement claims.

1. The ‘967 Patent

The ‘967 patent (“Method and system for distributing electronic tickets with visual display”), with a priority date of March 11, 2011, describes a novel system and method for distributing electronic tickets such that the ticket is verified at the entrance to venues by means of an animation or other human-perceptible “visual validation display object” that is selected by the venue for the particular event. (Appx85 Abstract.) This novel system and method removes the need for a ticket taker to use a barcode scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders. (Appx85.) Barcode scanners were not designed to read a lit LCD screen displaying a barcode. The reflectivity of the screen can defeat the scanning process. (Appx103 1:32-37.)

The '967 patent specification states that use of barcode scanners is impractical for the potential large crowds that often attend open venues and may be impracticable since barcode scanners are not highly compatible with LCD screen displays. (Appx103 2:16-22.) Considerable time, expense, and consumer frustration is involved in processing an electronic ticket, especially when the LCD display does not scan at all and a passenger has to be sent away to get a paper printout of a ticket. (Appx103 2:17-21.) The specification exclusively describes the invention as one in which a human verifies a ticket's authenticity without using a barcode scanner. (Appx103 1:15-20, 1:38-43, 2:17-21.)

The '967 patent addresses the problems of the prior art with "visual validation display objects," which are easily recognizable for users to present at the entrance to a venue. (Appx103 2:45-57.) The '967 patent further discloses the use of "tokens" to maintain the security of the "visual validation display objects" and other data stored in a data record. (Appx106 7:20-41.) The '967 patent additionally provides that the tokens authenticate a previously purchased ticket by determining whether a token associated with the previously purchased ticket has been stored in a data record associated with a received request, and if it has, whether the received token is valid. (Appx109 14:17-27.)

The claims of the '967 patent disclose that a previously purchased electronic ticket is verified according to an ordered combination of steps. (Appx109-111.)

First, a request is received from a user's computer device to verify purchase of a previously purchased electronic ticket and to obtain a visual validation display object. (Appx109-111.) Second, a token associated with the received request is received from the user's computer device. (Appx109-111.) Third, a determination is made if a token associated with a purchased electronic ticket has been stored in a data record associated with the request to verify a previous purchase. (Appx109-111.) Fourth, if a token associated with a purchased electronic ticket has been stored in a data record it is determined whether the token associated with the received request is valid. (Appx109-111.) Fifth, in dependence on the determination that the token associated with the received request is valid, the server system causes an activation of the previously purchased electronic ticket by transmitting to the user's computer device a data file comprising the visual validation display object. (Appx109-111.) This removes the need for the ticket taker to be involved in the authentication of the previously purchased ticket. Instead, that ticket taker may easily and quickly rely on the presence of the validation display object to verify the possession of an authentic previously purchased electronic ticket. (Appx109-111.)

2. The '993 Patent

The '993 patent ("Method and system for distributing electronic tickets with visual display"), with a priority date of March 3, 2011, was issued on January 19,

2016, after the U.S. Supreme Court’s decision in *Alice Corp. v. CLS Bank International* (2014). (Appx112.) It shares the same specification as the ‘967 patent. (Appx112-138.) As noted in the USPTO’s Notice of Allowance (May 23, 2016), the claims of the ‘993 patent were scrutinized both by the Examiner and a “[§] 101 expert, Jim Trammell.” (Appx3406.) That is, the USPTO brought in an expert to assess § 101 issues and confirm that the claims were patent-eligible.

The ‘993 patent describes a novel system and method for distributing electronic tickets such that the ticket is verified at the entrance to venues by means of an animation or other human-perceptible validation display object that is selected by the venue for the specific event. (Appx112 Abstract.) This novel system and method removes the need for a ticket taker to use a barcode scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders. (Appx112.)

The ‘993 patent addresses the problems of the prior art with “validation display objects,” which are easily recognizable for users to present at the entrance to a venue. (Appx131 1:27-46.) The ‘993 patent discloses the securing of a validation display object and ways in which the validation display object is secured against tampering. (Appx133 5:22-6:32, Appx137 14:23-24.) The ‘993 patent further discloses the use of “tokens” to maintain the security of the validation display objects. (Appx134 7:26-47.) The ‘993 patent additionally provides that the tokens

authenticate a previously purchased ticket by validating (or matching) a token received from the user's device to a stored token. (Appx134.) Upon validation of the token, by matching, the validation display object is either enabled or prevented (in the case of the token not matching) from being displayed. (Appx134.)

The claims of the '993 patent state that a previously purchased electronic ticket is verified according to an ordered combination of steps. First, a token—which is a unique alphanumeric string—associated with a previously purchased electronic ticket is transmitted to a user's remote display device. (Appx137 14:13-15.) Second, a copy of the unique alphanumeric string is stored on a central computer system. (Appx137 14:15-17.) Third, the token is validated by matching the token transmitted to the remote display device to the copy of the unique alphanumeric string stored on the central computing system to provide a ticket payload to the remote display device. (Appx137 14:18-22.) Fourth, claim 1 of the '993 patent recites securing a validation display object prior to transmission to provide a secured validation display object. (Appx137 14:23-24.) Fifth, the secured validation display object associated with the ticket payload is transmitted to the remote display device. (Appx137 14:25-27.) Sixth, the remote device is either enabled to display the secured validation display object upon validation of the token for visual recognition by the ticket taker or is prevented from displaying the secured validation display object if the token is not validated. (Appx137 14:28-33.)

This removes the need for the ticket taker to be involved in the authentication of the previously purchased ticket by use of a scanning machine. (Appx112.) Instead, that ticket taker may easily and quickly rely on the presence of the validation display object to verify the possession of an authentic previously purchased electronic ticket. (Appx131.)

B. Litigation of the Patents-in-suit

1. Litigation in the Eastern District of Texas

On May 20, 2016, Bytemark sued Masabi in the United States District Court for the Eastern District of Texas for willful infringement of the ‘967 patent and the ‘993 patent. *See Bytemark, Inc., v. Masabi Ltd.*, Civ. No. 2:16-cv-00543 (E.D. Tex.). Bytemark alleged that Masabi was using, offering for sale, and selling its visual validation mobile ticketing applications and systems that infringe at least claims 1, 2, 3, 4, 5, 6, 17, 18, 19, 20, 21, 22, 23, and 34 of the ‘967 patent literally and/or under the doctrine of equivalents, and at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 22, 23, and 24 of the ‘993 patent literally and/or under the doctrine of equivalents. (Appx5942-5943.) According to Bytemark’s complaint, Masabi sold and offered for sale its infringing visual validation applications and systems to entities throughout the United States, including the Massachusetts Bay Transportation Authority (“MBTA”) in Boston, the Southern California Regional Rail Authority (“Metrolink”) in Los Angeles, the Dallas Area Rapid Transit

(“DART”), and the New Orleans Regional Transit Authority (“RTA”). (Appx5943-5944.)

On October 4, 2017, Masabi filed a motion for summary judgment of invalidity under § 101 and other grounds—its first challenge to the validity of the patents-in-suit.¹ (Appx3193-3241.) Bytemark filed its opposition brief on October 20, 2017, addressing the arguments that Bytemark had made in its Motion. (Appx3244-3283.)

Four days later, before Masabi ever filed a reply brief, the district court removed the case from the December 4, 2017 docket, stating only that the trial date and all unexpired deadlines would be reset at a status conference on December 11, 2017—which the court subsequently canceled, to be reset by a future order.² (Appx3448.) On February 14, 2018, the court *sua sponte* issued an order staying the case pending further order. (Appx3452.) The district court provided no explanation for why it had stayed the case. (Appx3452.) On March 29, 2018, Bytemark filed an opposed motion for status conference. (Appx3453-3455.) The district court denied this motion on May 17, 2018, citing its broad discretion to stay proceedings as an incident to its power to control its own docket and stating that the case “remain[ed]

¹ Masabi never filed a motion to dismiss on any validity or patentability ground.

² Masabi filed a notice of institution of *inter partes* review later that same day (after the court had issued its notice). (Appx3449.) On January 26, 2018, Masabi filed a notice of third-party CBM petitions.

stayed in part because of pending proceedings at the Patent Trial and Appeal Board concerning the invalidity of the patents-in-suit.” (Appx3456.)

On November 26, 2018, more than one year after Masabi filed its motion for summary judgment and with no further summary judgment briefing having taken place, the magistrate judge issued an R&R recommending that Masabi’s Motion be granted and that the patents-in-suit be invalidated. (Appx3457-3474.) The district court summarily adopted the R&R on February 7, 2019, determining that no reasonable jury could find the claims of the patents patent-eligible. (Appx1.) In its opinion, the district court did not articulate what evidentiary standard it had relied upon, nor did it discuss whether or how Masabi had shown by clear and convincing evidence that the asserted claims of the patents-in-suit were invalid. (Appx3457-3474.) The district court referenced pending office actions of patents other than the patents-suit (none of which had been raised by either party), and stated that although “the claims at one time may have passed the § 101 filter[,] . . . under the law as it stands today, the asserted claims are not patent-eligible.” (Appx3473-3474, Appx3457-3474.) The district court did not cite any case decided after 2017 in its opinion. (Appx3457-3474.)

2. Litigation in other venues

Bytemark currently has two other pending lawsuits involving the patents-in-suit. On March 10, 2017, Bytemark sued defendants Xerox Corp., ACS Transport

Solutions, Inc., Xerox Transport Solutions, Inc., Conduent Inc., and New Jersey Transit Corp. in the Southern District of New York. *See Bytemark v. Xerox et al.*, Civ. No. 1:17-cv-01803 (S.D.N.Y.). Bytemark alleged, *inter alia*, infringement of the ‘967 and ‘993 patents. *Id.* The defendants in that case filed a motion to dismiss the patent infringement claims on the basis that the patents-in-suit were ineligible under § 101. *Id.* In a pre-motion conference held on October 16, 2017, the district court stated that “[t]he patents suggest an ‘arguably inventive device or technique for displaying information’ in response to ‘a problem specifically arising in’ the mobile technology field” and that Bytemark “ha[d] likely pled a sufficiently inventive concept to survive a motion to dismiss.” (Appx3440.) In light of this pending appeal, the patent claims in that case have been dismissed without prejudice by stipulation of the parties.

Additionally, on June 1, 2018, Bytemark sued defendant Token Transit, Inc. in the District of Delaware, alleging infringement of the ‘967 and ‘993 patents. *See Bytemark v. Token Transit, Inc.*, Civ. No. 1:18-cv-00834 (D. Del.). That case was stayed pending this appeal at the request of both parties on December 17, 2018.

3. Proceedings before the PTAB

The patents-in-suit have survived two covered business method patent reviews (CBMs), and claims 2 and 19 of the ‘967 patent³ survived an *inter partes* review (IPR) before the PTAB. On January 1, 2018, third parties Xerox et al. filed a petition for CBM review of the ‘967 patent (CBM2018-00011). (Appx5951-6048.) In their petition, Xerox et al. argued, *inter alia*, that the ‘967 patent was invalid for being directed to patent-ineligible subject matter under § 101. (Appx6007-6023.) Bytemark filed a preliminary response to the petition on April 27, 2018. (Appx5893.) Meanwhile, on January 15, 2018, third parties Xerox et al. filed a petition for CBM review of the ‘993 patent (CBM2018-00018). (Appx6049-6152.) In their petition, Xerox et al. similarly argued, *inter alia*, that the ‘993 patent was invalid for being directed to patent-ineligible subject matter under § 101. (Appx6112-6131.) Bytemark filed a preliminary response to the petition on April 27, 2018. (Appx5872.) On July 12, 2018, the PTAB declined to institute both of Xerox et al.’s CBM petitions, holding that the patents were not CBM patents pursuant to the statutory definition. (Appx5871-5913.) On August 21, 2018, the PTAB denied Xerox et al.’s request for rehearing involving the ‘967 patent.

³ The Board found that claims 1, 3-6, 17, 18, 20-23, and 34 are anticipated by the prior art. Bytemark has appealed that decision to this Court. *See Bytemark, Inc. v. Masabi Ltd.*, No. 19-1442 (Fed. Cir.).

(Appx5914-5926.) Likewise, on November 20, 2018, the PTAB denied Xerox et al.’s request for rehearing involving the ‘993 patent. (Appx5927-5940.)

Additionally, two claims of the ‘967 patent survived an IPR brought by Masabi on May 18, 2017 (IPR2017-01449). In its petition, Masabi argued that the patent’s claims were invalid because they were anticipated by the prior art. (Appx3.) On December 3, 2018, the PTAB issued its final written decision, holding that claims 2 and 19 of the ‘967 patent were patentable. (Appx2-66.) Bytemark filed a notice of appeal to this Court on January 18, 2019, and that case is currently pending before the Court. *See Bytemark, Inc. v. Masabi Ltd.*, No. 19-1442 (Fed. Cir.).

SUMMARY OF ARGUMENT

This is an appeal from a final judgment of the Eastern District of Texas granting Masabi’s motion for summary judgment of invalidity and invalidating all claims of the patents-in-suit.

In its Motion, Masabi incorrectly argued that the burden was on Bytemark and its expert to prove that the patent claims were valid (where an issued patent enjoys the presumption of validity) and failed to apply this presumption and present “clear and convincing” evidence of invalidity. Further, Masabi’s arguments were directed only towards claim 1 of each patent, and Masabi conclusorily argued that the dependent claims were similar without any support or reasoning.

In reaching its decision invalidating the patents-in-suit, the district court relied on the premise that although the ‘993 patent—which shares the specification of the ‘967 patent—previously overcame § 101 scrutiny by the examiner and a § 101 expert, “under the law as it stands today, the asserted claims are not patent-eligible.” Relying on the *Alice/Mayo* two-part test for subject matter eligibility, the district court first determined that, based on the record and pending patent applications, “the claims are directed to the abstract idea of verifying the authenticity of a ticket.” In the first step, the district court stated that it “f[ound] no relevant disputed underlying facts in this case, nor has Plaintiff demonstrated any.”

In step two, the district court concluded that “in light of the step one analysis, . . . the asserted claims do not include an inventive concept sufficient to move the claims away from the abstract idea.” According to the district court, “the claims, specification, and prosecution history all suggest that the concept recited in the claims is nothing more than using these conventional tools to verify the authenticity of an electronic ticket.”

The district court’s decision contains numerous errors that compel reversal by this Court. First, the district court erred in its conclusion that there is no genuine issue of material fact as to whether the claimed inventions are patent-eligible subject matter. Although the parties presented competing factual evidence, the district court failed to apply the controlling law, which states that the question of whether a claim

element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact that must be proven by clear and convincing evidence. Additionally, the district court failed to hold Masabi—the moving party—to its summary judgment burden, and impermissibly relied on arguments and issues that were outside the parties’ briefing. Further, the district court failed to limit Masabi’s arguments to claim 1 of the ‘967 patent and claim 1 of the ‘993 patent. This was error, as Masabi failed to meet its burden of establishing that claim 1 was representative, and its Motion wholly failed to discuss any dependent claims or distinct claim limitations of the dependent claims (despite Bytemark identifying such claims and claim limitations) or support why all of the asserted claims should be treated the same.

Additionally, the district court erred in its determination that the patent claims are subject-matter ineligible under § 101 as a matter of law. The district court’s opinion, which issued in 2019 and contended that the asserted claims would no longer be patent-eligible under “current law,” failed to cite a single *Alice* case post-2017, including relevant cases decided by this Court. Under the existing law, the claims of the patents-in-suit are subject-matter eligible as a matter of law.

Given these widespread errors, Bytemark requests that the district court’s decision be reversed in its entirety.

STANDARD OF REVIEW

This Court applies the law of the regional circuit when reviewing summary judgment decisions. *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 761 F.3d 1329, 1337 (Fed. Cir. 2014) (citing *Lexion Med., LLC v. Northgate Techs., Inc.*, 641 F.3d 1352, 1358 (Fed. Cir. 2011)). The Fifth Circuit reviews the district court’s grant of summary judgment de novo. *Smith v. Reg’l Transit Auth.*, 827 F.3d 412, 417 (5th Cir. 2016). As such, this Court will only affirm if there is no genuine dispute as to an issue of material fact, and the moving party is entitled to summary judgment as a matter of law. *Id.* (citing Fed. R. Civ. P. 56(a)); *Amdocs*, 761 F.3d at 1337-38. Further, when reviewing a motion for summary judgment, this Court “must view the evidence introduced and all factual inferences from the evidence in the light most favorable to the party opposing summary judgment.” *Smith*, 827 F.3d at 417. “[B]ecause a patent carries a presumption of validity and a challenger must prove invalidity by clear and convincing evidence, a patentee need not present *any* factual evidence to prevail on a motion for summary judgment of validity.” *Cap Exp., LLC v. Zinus, Inc.*, 722 F. App’x 1004, 1008 (Fed. Cir. 2018) (citing *Massey v. Del Labs., Inc.*, 118 F.3d 1568, 1573 (Fed. Cir. 1997)).

A district court’s grant of summary judgment of invalidity under § 101 is reviewed de novo. *Roche Molecular Sys., Inc. v. CEPHEID*, 905 F.3d 1363, 1368 (Fed. Cir. 2018); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1352 (Fed.

Cir. 2016). Section 101 defines patent-eligible subject matter as “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.”⁴ 35 U.S.C. § 101. Although whether a claim is directed to statutory subject matter is a question of law, the § 101 inquiry may contain underlying issues of fact. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018) (citing *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1325 (Fed. Cir. 2016)). “The question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact.” *Id.*

⁴ To determine whether a patent claims ineligible subject matter, this Court follows a two-step framework. First, the Court determines whether the claims at issue are directed to a patent-ineligible concept such as an abstract idea. *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 217 (2014). Second, if the claims are directed to an abstract idea, the Court “consider[s] the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 556 U.S. 66, 79 (2012)).

ARGUMENT

A. The District Court’s Grant of Summary Judgment Was Error Because There Is a Genuine Issue of Material Fact As to Whether The Claimed Inventions Are Patent-Eligible Subject Matter.

1. Whether a claim element or combination of elements is well-understood, routine and conventional is a question of fact that must be proven by clear and convincing evidence.

“The question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact.” *Berkheimer*, 881 F.3d at 1368. “Any fact, such as this one, that is pertinent to the invalidity conclusion must be proven by clear and convincing evidence.” *Id.* Further, “deference must be given to the determination made by the fact finder on this issue.” *Exergen v. KAZ USA Inc.*, 725 Fed. App’x 959 (Fed. Cir. 2018). “Because the patent challenger bears the burden of demonstrating that the claims lack patent eligibility, . . . there must be evidence supporting a finding that the additional elements were well-understood, routine, and conventional.” *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1356 (Fed. Cir. 2018). “As this is a factual question, the normal procedural standards for fact questions must apply, including the rules in the Federal Rules of Civil Procedure applicable to motions . . . for summary judgment.” *Id.* “If there is a genuine dispute of material fact, Rule 56 requires that summary judgment be denied.” *Id.* at 1357.

In its decision, the district court made no reference to any of these legal standards.⁵ In its brief analysis of the inventive concept inquiry (step two of the *Alice* test), the district court made no mention of the factual evidence put forth by the parties—including the competing testimony of the parties’ technical experts as to whether the claims are well-understood, routine and conventional. (Appx3472-3473.) Instead, the district court appears to have improperly treated the inventive concept analysis as if it were not a fact question at all. (Appx3472-3473.) Based on the controlling law, this was error. *See Berkheimer*, 881 F.3d at 1368.

Additionally, the district court failed to place the burden on Masabi to demonstrate that the claims lack patent eligibility and that no reasonable jury could find that the claim elements are not well-understood, routine, and conventional. *See Aatrix Software*, 890 F.3d at 1356-57. It is also apparent that the district court did not begin with the presumption that the patents-in-suit are valid⁶ and require that

⁵ Although the above cases had not been decided at the time of the parties’ briefing, they had been decided by the time the district court issued its decision, and the relevant law was raised by Bytemark in its objections to the magistrate judge’s R&R. (Appx6157-6158.)

⁶ “This statutory presumption derives in part from recognition of the technological expertise of the patent examiners.” *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1139 (Fed. Cir. 1985). “In litigation, where a patentee cannot amend his claims, or add new claims, the presumption, and the rule of claim construction (claims shall be construed to save them if possible), have important roles to play.” *In re Etter*, 756 F.2d 852, 858-59 (Fed. Cir. 1985). Further, “[t]he Examiner’s decision . . . is . . . evidence the court must consider in determining whether the party

Masabi prove invalidity with clear and convincing evidence. *See Berkheimer*, 881 F.3d at 1368. Not only did the district court fail to cite any evidence put forth by Masabi that would meet the “clear and convincing” standard, the district court effectively dismissed the USPTO’s determination that the patents-in-suit were valid because the ‘993 patent issued “only six months” after the *Alice* decision (Appx3470-3471),⁷ and impermissibly shifted the burden of proving validity to Bytemark. *See Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1359-60 (Fed. Cir. 2007) (“Th[e] burden of proof never shifts to the patentee to prove validity.”); *In re Etter*, 756 F.2d 852, 856 (Fed. Cir. 1985) (“[T]he presumption require[s] the decisionmaker “to employ a decisional approach that starts with the acceptance of the patent claims as valid and that looks to *the challenger* for proof of the contrary.”).

In fact, “because a patent carries a presumption of validity and a challenger must prove invalidity by clear and convincing evidence,” Bytemark did not need to “present *any* factual evidence to prevail on a motion for summary judgment of validity.” *Cap Exp.*, 722 F. App’x at 1008 (citation omitted).

asserting invalidity has met its statutory burden by clear and convincing evidence.” *Interconnect Planning*, 774 F.2d at 1139.

⁷ The district court stated, “Bytemark emphasizes that the applicant overcame this rejection [of the ‘993 patent], and that the examiner even made the rare decision to consult a ‘101 expert’ before allowing the claims. But the Supreme Court had issued the *Alice* decision only six months before the claims were allowed, and the reach of *Alice* was not yet understood.” (Appx3470-3471.)

The district court's failure to apply the correct legal standards was error, and, as discussed further below, this error was determinative.

2. A reasonable jury could find that the claim elements of the patents-in-suit are not well-understood, routine, and conventional.

The district court erred in holding that there are no relevant disputed underlying facts in this case. The framework for determining whether a claim is eligible for patenting was formulated in *Alice* as a two-step analysis, whereby it is first determined whether the claimed subject matter is directed to an abstract idea. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). If so, the second step involves determining whether the elements of the claim, considered “both individually and as an ordered combination,” contain an “inventive concept.” *Id.* To constitute an inventive concept at step two, elements of a patent must be more than “well-understood, routine, conventional activity.” *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 556 U.S. 66, 79 (2012); *In re Morinville*, No. 2018-1895, 2019 WL 1890529, at *3 (Fed. Cir. Apr. 29, 2019).

The question of whether such elements (or their combination) are well-understood, routine, and conventional to a skilled artisan in the relevant field is a question of fact, and deference must be given to the determination made by the fact finder on this issue. *Exergen Corp.*, 725 F. App'x at 965; *Berkheimer*, 890 F.3d at 1370 (“Whether a claim element or combination of elements would have been well-

understood, routine, and conventional to a skilled artisan in the relevant field at a particular point in time may require “weigh[ing] evidence,” “mak[ing] credibility judgments,” and addressing “narrow facts that utterly resist generalization.”); *see also Uniloc USA, Inc. v. Samsung Elecs. Am., Inc.*, No. 2:17-CV-00651-JRG, 2018 WL 4927279, at *2 (E.D. Tex. Sept. 18, 2018) (“The question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact [**that must] be proven by clear and convincing evidence.**”) (emphasis added). Indeed, the issue of whether claims of a patent contain an “inventive concept” has been treated by district courts as an issue to be resolved at trial. *Maxwell, Ltd. v. ZTE (USA) Inc.*, 5:16-cv-00179-RWS, Dkt. No. 228 (E.D. Tex. June 29, 2018); *Finjan, Inc. v. Juniper Network, Inc.*, No. C 17-05659 WHA, 2018 WL 4184338, at *11 (N.D. Cal. Aug. 31, 2018) (holding on summary judgment that “the Court will wait to have the benefit of the trial record before determining whether Claim 10 contains an inventive concept such that it is patent eligible”).

In its Opposition, Bytemark specifically disputes Masabi’s argument that the asserted claims fail to recite an inventive concept and identifies supporting factual evidence that makes finding Bytemark’s patents subject matter ineligible improper

on summary judgment.⁸ For example, relying on its expert Dr. Gottesman, Bytemark explains how the specific use of a token as disclosed and claimed in Bytemark's patents is non-conventional and innovative. (Appx2781-2782.) Dr. Gottesman testifies that the claims of the patent-in-suit "involve[] a unique use of technology to improve the way servers and computers communicate with and transfer information with remote devices in the context of implementing a visual validation mobile ticketing system." (Appx2781-2782.) Dr. Gottesman further testifies that the use of a token as disclosed in the claims of the patents in suit provide non-conventional security protocols. (Appx2781-2782.) Dr. Gottesman also describes how the combination of claim elements taught by the asserted claims of the patents-in-suit is a new and useful improvement of existing technology that was not known at the time of invention and amounts to significantly more than the alleged abstract idea of merely distributing and visually validating electronic tickets. (Appx2730, Appx2781-2782.)

Dr. Gottesman also testifies regarding the state of the art at the time of the invention and the problems with the prior art that the patents-in-suit overcome.

⁸ Contrary to Masabi's assertion, Bytemark does not concede to patent-ineligible subject matter. Indeed, Bytemark challenges the paragraphs of Sigurd Meldal's (Masabi's expert witness) testimony. (Appx3259, Appx3261, Appx3264-3267.)

(Appx2730-2736.) For instance, in discussing the claim elements of the independent claims of the '967 patent, Dr. Gottesman testifies that

It was not known, prior to the '967 Patent, to have a previously purchased electronic ticket that is activated by [a server system] determining that a received token (which is associated with a request to verify purchase of the previously purchased electronic ticket) is valid and transmitting to the user's computer device a data file including the visual validation display object configured to be readily recognizable visually by a ticket taker.

(Appx2733.)

Dr. Gottesman testifies that the '967 and '993 patents provided an early solution to the need for distributing electronic ticketing in a practical, efficient and secure manner. (Appx2730.) Dr. Gottesman also testifies that the problem with prior art systems is that the computer scanning process is fraught with error, as barcode scanners were not designed to read a lit LCD screen displaying a barcode. (Appx2750-Appx2751.) The inventions disclosed and claimed in the '967 and '993 patents eliminated the need to use a barcode scanner on an LCD display of a cell phone or other device and improved the ticket verification process. (Appx2730, Appx2750-2751.)

Masabi concedes in its own literature describing its infringing system that claim limitations disclosed and claimed in Bytemark's patents are unconventional in nature. (Appx3263.) Relevant to dependent claims 12 and 13 of the '993 patent, which include the added limitation that "the remote display device displays the

secured validating display object without a network connection with the central computer system,” Masabi’s website highlights the unconventional nature of this particular technical feature. (Appx137 15:33-39, Appx3263.)

Additionally, in a parallel case addressing the § 101 eligibility issues related to the same claims of the ‘967 and ‘993 patents asserted here, the Southern District of New York found⁹ that “[t]he patents suggest an ‘arguably inventive device or technique for displaying information’ in response to ‘a problem specifically arising in’ the mobile technology field.” *Bytemark v. Xerox et al.*, 1:17-cv-01803-PGG, Dkt. No. 49 (SDNY); (Appx3438-3440.)

Whether a claim element is well-understood, routine, and conventional is a question of fact that Masabi and Bytemark dispute. Based on this evidence, a reasonable jury could find that the elements of the claims of the patents-in-suit “both individually and as an ordered combination” are not well understood, routine, and conventional, *see Alice Corp.*, 573 U.S. at 217, and the district court erred in wholly ignoring the factual dispute in this case without any explanation. Accordingly,

⁹ In a conference addressing the likelihood of success of Xerox’s § 101 challenge in *Bytemark v. Xerox et al.* in the Southern District of New York, Judge Paul Gardephe read into the record his opinion that “[t]he patents suggest an ‘arguably inventive device or technique for displaying information’ in response to ‘a problem specifically arising in’ the mobile technology field,” and concluded that “it appears to me that plaintiff has likely pled a sufficiently inventive concept.” (Appx3438-3440.)

summary judgment was not appropriate and this Court should reverse the district court's ruling.

3. In determining that summary judgment was proper, the district court impermissibly relied on argument and issues outside of the parties' briefing.

In its decision, the district court relied on statements made by examiners during the prosecution of “related patent applications.” (*See, e.g.*, (Appx3465-3466, Appx3470-3471.)) Although Masabi never mentioned these applications in its summary judgment briefing (nor did Bytemark), the district court cited these applications as key support for its conclusion that the patents-in-suit—which overcame scrutiny under § 101 and *Alice* when they were prosecuted—“cannot withstand scrutiny under current § 101 jurisprudence” (Appx3465-3466), and “under the law as it stands today, the asserted claims are not patent-eligible” (Appx3473-3474.).¹⁰ For example, in its analysis of whether the asserted claims are directed to an abstract idea, the district court cited the pending applications as evidence that the

¹⁰ *See, e.g.*, (Appx3469 (“The step one inquiry in this case could likely end with the claim language, but the specification and prosecution history support the conclusion that is evident from the claims.”)); (Appx3469-3470); (Appx3471 (“Notably, in the continuation applications that remain pending today, claims that arguably include greater technical detail than the asserted claims have been rejected by the Patent Office under more recent § 101 precedent.”)); (Appx3471-3472); (Appx3472-3473) (“[T]he claims, specification, and prosecution history all suggest that the concept recited in the claims is nothing more than using these conventional tools to verify the authenticity of an electronic ticket.”)).

claims of the patents-in-suit are ineligible subject matter under the current law, stating: “Notably, in the continuation applications that remain pending today, claims that arguably include greater technical detail than the asserted claims have been rejected by the Patent Office under more recent § 101 precedent.” (Appx3471.) The district court’s reliance on these pending applications—which were never raised or argued by either party—was error.

“In our adversary system . . . we rely on the parties to frame the issues for decision and assign to courts the role of neutral arbiter of matters the parties present.” *Greenlaw v. United States*, 554 U.S. 237, 243 (2008); *see also United States v. Green*, 508 F.3d 195, 203 (5th Cir. 2007) (holding that claim asserted in a single sentence at end of appellant’s opening brief, without further elaboration, was deemed waived for inadequate briefing). Although the district court may have believed that the pending applications provided a compelling reason to invalidate the patents-in-suit, the district court’s decision does not reflect the framing of either party.

Instead, the district court failed to assume the rule of “neutral arbiter” and made improper arguments on behalf of Masabi. None of Masabi’s arguments related to the pending patent applications or the arguments made therein. Masabi’s Motion was the “fram[ing] of the issues for decision” that Masabi chose and that the district court was bound to accept. *See Greenlaw*, 554 U.S. at 243. Moreover, the district

court's attempt to justify its reference to these patent applications—because “[for] much of the same reasons as the examiners have articulated in these related patent applications, Masabi argues that the asserted claims of the patents-in-suit cannot withstand scrutiny under current § 101 jurisprudence” (Appx3466)—is belied by Masabi's briefing. The reasonings cited in the pending applications were not the same or sufficiently comparable to the arguments made by Masabi.

Crucially, because the district court made new arguments on behalf of Masabi that were nowhere in Masabi's briefing, Bytemark never had a chance to respond to or address these arguments.¹¹ Bytemark was entitled to this minimum opportunity before being deprived of valuable property rights that are, and have been, the subject of extensive litigation and post-grant review in forums throughout the country. Because the district court's decision violates the fundamental “principle of party presentation,” *see id.*, its conclusions should be rejected.

4. The pending office actions are not final determinations and, in fact, support the validity of the patents-in-suit.

The district court's reliance on the pending office actions was also improper because the office actions are not final determinations. For example, in view of the newest § 101 guidelines and additional attorney argument, the USPTO has

¹¹ The magistrate judge issued his R&R after Bytemark submitted its opposition brief but before full briefing by the parties had been completed. Thus, the district court's order was decided based only on Masabi's motion for summary judgment and Bytemark's opposition to that motion.

withdrawn the § 101 rejection with respect to Application No. 14/286,622 (“Method and system for distributing electronic tickets with data integrity checking”). (Appx3603.) Likewise, the USPTO has withdrawn the § 101 rejection with respect to Application No. 14/823,157 (“Method and system for distributing electronic tickets with visual display for verification”), explaining that “[t]he analysis [is] in line with current 101 guidelines.” (Appx5218.) The USPTO indicated that claims 1 and 10 should be amended to recite limitations of claims 29 and 30. (Appx5218.) Application No. 14/597,965¹² (“Method and system for employing anti-ticket fraud system for mobile tickets”) is still awaiting an office action following Bytemark’s arguments and amendments. Thus, much of the reasoning cited and relied upon by the district court was premature, and did not represent the USPTO’s final determination on these issues.¹³

¹² The district court incorrectly identified the application number as 14/597,905.

¹³ For reasons such as these, courts have cautioned that non-final rejections of patent applications should not be “outcome determinative.” *See Univ. Secure Registry, LLC v. Apple Inc.*, No. CV 17-585-CFC-SRF, 2018 WL 4502062, at *12 (D. Del. Sept. 19, 2018). As this Court has explained, a “non-final rejection by the examiner is not an action from which legal consequences will flow.” *Mikkilineni v. Stoll*, 410 F. App’x 311, 313 (Fed. Cir. 2010). This is because after a non-final rejection, the applicant may reply to the rejection, and “the application or the patent . . . will be reconsidered and again examined.” 37 C.F.R. §§ 1.111-1.112. At the end of this back-and-forth process, the applicant may overcome the non-final rejection and receive a patent. *Mikkilineni*, 410 F. App’x at 313.

Moreover, even assuming the office actions *were* properly considered by the district court, because the USPTO ultimately determined that claims of these related patents (which share the specification of the patents-in-suit) are indeed § 101 eligible under the “the law as it stands today,”¹⁴ these pending applications *support*—not undermine—the validity of the patents-in-suit.

5. The Court Erred by Not Limiting Masabi’s Arguments to Claim 1 of the ‘967 Patent and Claim 1 of the ‘993 Patent.

The district court overreached in extending its holding to all asserted claims when Masabi’s failed to meet its burden of showing that claim 1 of the ‘967 patent and claim 1 of the ‘993 patent are representative claims. The movant bears the burden of showing that the other asserted claims are “substantially similar and linked to the same abstract idea” when relying on a representative claim in its section 101 analysis. *See Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343, 1348 (Fed. Cir. 2014); *Perdiemco, LLC v. Industrack LLC*, No. 2:15-CV-1216-JRG-RSP, 2016 WL 5719697, at *7 (E.D. Tex. Sept. 21, 2016), *report and recommendation adopted*, No. 2:15-CV-727-JRG, 2016 WL 5475707 (E.D. Tex. Sept. 29, 2016); *see also Uniloc USA, Inc. v. AVG Techs. USA, Inc.*, No. 2:16-CV-00393-RWS, 2017 WL 1154927, at *4 (E.D. Tex. Mar. 28, 2017); *Versata*

¹⁴ The USPTO’s determinations regarding Application No. 14/286,622 and Application No. 14/823,157 were made in 2019 and based on the law at that time.

Software, Inc. v. NetBrain Techs., Inc., No. 13-676-LPS-CJB, 2015 WL 5768938, at *4 (D. Del. Sept. 30, 2015). *Cf. ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 766 (Fed. Cir. 2019) (addressing each claim where the parties failed to designate a representative claim); *Cleveland Clinic Found. v. True Health Diagnostics LLC*, 859 F.3d 1352, 1358 (Fed. Cir. 2017), *cert. denied*, 138 S. Ct. 2621 (2018) (accepting Defendant’s “representative claim” where the “plaintiff fail[ed] to point out any claim that is not represented by the aforementioned claims.”)

Here, the district court’s conclusion that “the claims that depend from claims 1 and 8 of the ’993 patent, like the dependent claims of the ’967 patent, recite additional steps, but the essence of the invention is captured by the independent claims” is insufficient basis to find all asserted claims¹⁵ patent-ineligible. Masabi—not the district court—was required to demonstrate that claim 1 of the ’967 and claim 1 of the ’993 were representative of all asserted claims. Masabi failed to meet its burden. Indeed, Masabi’s Motion wholly fails to discuss any dependent claims or distinct claim limitations of the dependent claims or support why all of the asserted claims should be treated the same. Moreover, in its Opposition, Bytemark specifically shows how an exemplary claim (claim 13) adds the limitation “wherein the remote display device displays the secured validating display object *without a*

¹⁵ In its amended complaint, Bytemark asserts at least claims 1, 2, 3, 4, 5, 6, 17, 18, 19, 20, 21, 22, 23, and 34 of the ’967 patent and at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 22, 23, and 24 of the ’993 patent. (Appx5942-5943.)

network connection with the central computer system.” Additionally, Bytemark demonstrates that Masabi’s own website highlights this particular functionality, suggesting that it is important to customers and unconventional. (Appx3263.)

Case law cited by the district court is inapt. In *Content Extraction*, the plaintiff never asserted in its opposition motion that it disagreed with defendant’s argument (or the district court’s assessment) that certain claims were representative. 776 F.3d at 1348 (“If CET disagreed with PNC’s or the district court’s assessment, CET could have identified claims in its opposition brief that it believed would not be fairly represented by claim[] 1 . . . for purposes of PNC’s § 101 challenge.”). Here, Bytemark’s Opposition challenged Masabi’s reliance on representative claims and identified exemplary claims not fairly represented.

As Masabi provided no support for lumping all of the asserted claims together, it failed to meet its burden of establishing that claim 1 of the ‘967 and claim 1 of the ‘993 patent represent all of the claims, and the district court’s application of its holding to all asserted claims was in error. Accordingly, the Court should reverse the district court’s opinion with respect to claims 2-6, 17-23, and 34 of the ‘967 patent, and claims 2-17, and 22-24 of the ‘993 patent.¹⁶

¹⁶ The district court’s determination that the preemption inquiry is moot because the asserted claims “recite[] ineligible subject matter as defined by *Alice* and its progeny” (Decision at 17) was also erroneous. This conclusion is contradicted by the specifications and language of the claims. Contrary to the district court’s reasoning, preemption is the underlying concern that drives the § 101 analysis, *see*

B. Even if There Is No Genuine Issue of Material Fact, the Patent Claims Are Subject-Matter Eligible Under § 101 As a Matter of Law.

Even if the Court determines there is no genuine issue of material fact, the district court erred in determining that the asserted claims of the patents-in-suit are invalid as a matter of law because: (1) the claimed inventions are not directed towards an abstract idea; and (2) the ‘967 and ‘993 patents disclose an inventive concept. Section 101 of the Patent Act provides that a patent may be obtained for “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.” 35 U.S.C. § 101. Only three narrow exceptions to the broad patent-eligibility principles of § 101 exist: “laws of nature, physical phenomena, and abstract ideas.” *Bilski v. Kappos*, 561 U.S. 593, 601-02 (2010) (“*Bilski IP*”). To determine whether a patent claims ineligible subject matter, the Supreme Court has established a two-step framework. *Alice Corp.*, 573 U.S. at 217; *see also SRI Int’l, Inc. v. Cisco Sys., Inc.*, 918 F.3d 1368, 1374 (Fed. Cir. 2019).

Alice, 134 S. Ct. at 2354, and courts have often cited the lack of preemption concerns to support a determination that a claim is patent-eligible under § 101, *see, e.g., McRO, Inc. v. Bandai Namco Games Am., Inc.*, 837 F.3d 1299, 1315-16 (Fed. Cir. 2016) (finding that the challenged claim would not foreclose “future alternative discoveries” and that “[t]he claim uses the limited rules in a process specifically designed to achieve an improved technological result in conventional industry practice”); *see also Alice*, 134 S. Ct. at 2354. Here, the challenged claims “use[] the limited rules in a process specifically designed to achieve an improved technological result in conventional industry practice” and would not foreclose “future alternative discoveries.” *See McRO*, 837 F.3d at 1315-16.

First, a court determines whether the claims at issue are directed to a patent ineligible concept. *Alice Corp.*, 573 U.S. at 216. If this threshold determination is met, the court moves to the second step of the inquiry and “considers the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Id.* (quoting *Mayo*, 566 U.S. at 78).

The appropriate analysis of whether a claim satisfies § 101 requires viewing the claim as a whole and not individual limitations. *Diamond v. Diehr*, 450 U.S. 175, 188-89 (1981); *King Pharms., Inc. v. Eon Labs, Inc.*, 616 F.3d 1267, 1277 (Fed. Cir. 2010) (“The Supreme Court has stated that a § 101 patentability analysis is directed to the claim as a whole, not individual limitations.”).

1. The district court erroneously concluded that the claimed inventions of the ‘967 and ‘993 patents are directed towards an abstract idea.

The district court erred in holding that the claimed inventions of the ‘967 and ‘993 patents are directed towards an abstract idea. A claim is not directed to an abstract idea where “the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer[s].” *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014); *see also Trading Techs. Int’l, Inc. v. CQC, Inc.*, 675 Fed. App’x 1001,

1004-05 (Fed. Cir. 2017); *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1257 (Fed. Cir. 2017).

This Court instructs that when a claim improves computer functionality and/or a technological process, the claim passes step one of *Alice* and is patent eligible. *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1007 (Fed. Cir. 2018); *Core Wireless Licensing S.A.R.L. v. LG Electronics, Inc.*, 880 F.3d 1356, 1363 (Fed. Cir. 2018); *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1344 (Fed. Cir. 2018), *as amended* (Nov. 20, 2018); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1334-35 (Fed. Cir. 2016). Further, a patent specification's disparagement of the prior art is relevant to determining the scope of the invention and the differences of the invention with respect to the prior art. *Enfish*, 822 F.3d at 1337 (citing *Openwave Sys. Inc. v. Apple Inc.*, 808 F.3d 509, 513-14 (Fed. Cir. 2015)). For example, in *Enfish*, this Court noted that "the claims are directed to an improvement of an existing technology [that] is bolstered by the specification's teachings that the claimed invention achieves other benefits over conventional databases, such as increased flexibility, faster search times, and smaller memory requirements." *Id.*

Similarly, in *Ancora Technologies*, this Court held that the claimed advance was a concrete assignment of specified functions among a computer's components to improve computer security and was therefore eligible for patenting. 908 F.3d at 1344. There, the patent described the flaws of prior art software and hardware

solutions to the identifying and restricting of an unauthorized software program's operation. *Id.* It also described an asserted improvement to the prior art solutions based on assigning certain functions to particular computer components and having them interact in specified ways. *Id.* at 1344-45. In finding the claims patent eligible, this Court held that “improving security—here, against a computer’s unauthorized use of a program—can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem.” *Id.* at 1348.

a. The claims of the ‘967 and ‘993 patents improve a technological process.

The present invention is similar to those in *Enfish* and *Ancora Technologies*. As in *Enfish*, the present invention improves prior art technology by removing the need for a barcode scanner (which is slow and prone to scanning problems when used on an LCD screen), while invoking discrete technological improvements to ensure security and avoid ticketing piracy issues. For example, the specification of the patents-in-suit describes that:

Venues such as theaters, amusement parks and other facilities that use tickets, for example airlines, ferries and other transportation have a need to use electronic ticketing. Existing systems distribute information that can constitute a ticket, but the verification problem is difficult. In one example of prior art, an electronic ticket is displayed as a bar-code on the recipient’s telephone display screen. The telephone is then placed on a scanner that reads the bar-code in order to verify the ticket. The problem with these systems is that the scanning process is fraught with error and the time taken to verify the electronic

ticket far exceeds that of the old system: looking at the paper ticket and tearing it in half. Barcode scanners were not designed to read a lit LCD screen displaying a bar code. The reflectivity of the screen can defeat the scanning process. Therefore, there is a need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket. This invention provides for the distribution of an electronic ticket that also contains a visual display that ticket takers can rely on as verification, without using a scanning device.

(Appx103 1:24-43, Appx131 1:29-48.)

Further, as in *Ancora Technologies*, the claims of the ‘967 and ‘993 patent improve security through a specific technique that solves computer specific problems in the prior art. The claims of the Bytemark patents disclose a specific non-abstract technique for identifying and preventing attempted fraudulent/unauthorized use of electronic tickets at the server level (i.e., without the use of a machine such as a barcode scanner). The specification identifies security problems associated with prior art electronic ticketing and paper ticketing and describes in detail how the invention overcomes those problems. (Appx105-107 5:16-10:4.) For example, the specification states that “the ticket payload can be **secured in a region of the device** under the control of the telecommunications provider [so that] the customer cannot access the code compromising the ticket payload.” (Appx105 5:28-31) (emphasis added). The specification also describes a technological solution that deters piracy. (Appx105 6:48-59.) The specification provides: “security can also be enhanced by retaining as steganographic data

embedded in the validating visual object” and that the “application can be operated to recover that information and display it on the screen [so that] suspicious ticket holders can be subjected to increased scrutiny.” (Appx105 6:48-59.)

The claims provide further support. For instance, claim 1 of the ‘967 patent solves ticket validation and authentication issues (that previously necessitated the use of a barcode scanner). Claim 1 teaches that the server system first “receives from the user’s computer device a token associated with the received request.” (Appx109 14:14-16.) Next, the server system “determines whether the token associated with the received request has been stored in a data record associated with the received request.” (Appx109 14:17-20.) Then, if it has, “**whether the received token is valid.**” (Appx109 14:17-20) (emphasis added). Only if the token is valid, the server system “caus[es] an activation of the purchased electronic ticket by transmitting to the user’s computer device a data file comprising the visual validation display object.” (Appx109 14:21-27.)

The dependent claims provide additional details about the claimed technical improvement necessary to solve the piracy problems identified in the patents. For instance, claim 3 of the ‘967 patent recites the storage of “data value” in a particular location: “storing **in the data record** associated with the purchased electronic ticket **a data value** representing a predetermined lock time.” (Appx109 14:41-51) (emphasis added). Accordingly, the claimed invention invokes a technical solution

to overcome problems arising from the technology previously used to implement mobile ticketing.

b. The district court erred by focusing on claim elements in isolation and oversimplifying the claimed inventions.

The district court erred by considering claim elements in isolation and oversimplifying Bytemark's inventions when comparing the instant facts to previous precedent. First, the district court's focus on hardware (e.g., "servers" and "computer device[s]") and "software or data elements" ("visual validation object," "token," and electronic ticket") in isolation, untethered from the disclosure of the claims and teachings of the specification, was in error. (Appx3468-3469.) Particularly, in the case of the claimed "token," the district court oversimplifies the inventions by focusing on what the token is rather than the functionality of the token as recited and claimed by the claims of the patents-in-suit. (Appx3468.) For example, the district court stated that "[t]he 'token' is a number, and the use of tokens, or 'tokenization' was well known long before the priority dates of these asserted claims." (Appx3468.) The district court further stated, "[T]he use of 'tokens' in a computer environment is not a technological improvement, but rather 'much like the identification of a coin or token as genuine in a mechanical transit

system toll device.’”¹⁷ (Appx3468.) Contrary to the district court’s understanding of Bytemark’s invention, it is the ordered combination of the claim elements that is the essence of the invention and allows the server system to provide validation of a token and authentication of a ticket without additional hardware (i.e., a barcode scanner). For instance, the ‘967 patent discloses that tokens are used to maintain the security of the “visual validation display objects” and other data stored in a data record. (Appx106 7:20-41.) The ‘967 patent additionally provides that the tokens authenticate a previously purchased ticket by determining whether a token associated with the previously purchased ticket has been stored in a data record associated with a received request, and, if it has, whether the received token is valid. (Appx109 14:17-27.)

Second, the facts of the cases¹⁸ relied upon by the district court are inapposite. In *Intellectual Ventures*, the district court found the patent-at-issue was directed

¹⁷ Citing *Smart Sys. Innovations, LLC v. Chi. Transit Auth.*, 873 F.3d 1364 (Fed. Cir. 2017).

¹⁸ The district court relies on the premise that even though “the claims one time may have passed the § 101 filter[,] under the law as it stands today, the asserted claims are not patent-eligible.” The district court issued its opinion on February 7, 2019, yet does not cite to any cases after 2017 including the following cases relevant to this dispute: *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343 (Fed Cir. 2018); *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); and *Berkheimer v. HP Inc.*, 881 F.3d 1360 (2018). Contrary to the district court’s conclusion, the asserted claims of the patents-in-suit enjoy a presumption of validity and remain patent eligible “under the law as it stands today” (as of May 6, 2019). Nevertheless, the cases relied upon by the district court are inapposite.

towards the abstract idea of “tracking financial transactions to determine whether they exceed a pre-set spending limit (i.e., budgeting)” and that increasing the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea. *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1367, 1370 (Fed. Cir. 2015). Similarly, the Federal Circuit held that the inventions in *Smart Systems* were directed at “the formation of financial transactions in the mass transit industry and data collection related to such transactions,” and rejected the appellant’s argument that the claims were patent-eligible because they improved prior systems “by speeding up the process at the turnstyle.” *Smart Sys. Innovations, LLC v. Chi. Transit Auth.*, 873 F.3d 1364, 1372 (Fed. Cir. 2017).

In this case, the district court oversimplifies Bytemark’s inventions. Unlike in *Intellectual Ventures* and *Smart Systems*, the claims are not directed towards a financial transaction. Indeed, in denying Masabi’s CBM patent reviews involving each of the patents-in-suit, the PTAB held that the patents-in-suit do not perform data processing or other operations used in the practice, administration, or management of a financial product or service. (Appx5886-5889, Appx5905-5907.) The district court’s characterization of the claims as being directed towards “security of . . . financial transaction[s]” (Appx3472) and “collecting, storing, recognizing, and manipulating data, or encoding or decoding data, to make the data human-or machine-readable” (Appx3471) fails to properly acknowledge key solutions such as

avoiding piracy and fraud (e.g., (Appx133 6:54-65, Fig. 13b)) and improving server system communication (e.g., (Appx134 8:36-54)), among others.

Additionally, unlike in *Smart Systems*, where the inventions involved long-existing technology (bank cards) being used in a conventional manner (providing bankcard data) to validate entry into a transit system, *Smart Sys.*, 873 F.3d at 1372-73, the inventions disclosed and claimed in the '967 and '993 patents, as detailed above, involve using technology (including tokens as disclosed and claimed), such as mobile devices and server systems, in an unconventional manner to provide a tangible technological solution to the real-world problems of errors associated with traditional electronic ticketing (that depended on barcode scanners), and security and piracy/copying issues associated with pre-computer period ticketing, including paper ticketing.

Further, the dependent claims (not addressed at all by either Masabi or the district court) solve additional technological problems including those involving secure display of tickets when there is no network connection (e.g., (Appx138 15:33-39)) and facilitating the usage of purchased tickets across different devices by conducting an additional check for a purchased electronic ticket in the absence of a stored token associated with the electronic ticket (e.g., (Appx134 7:47-8:35, Appx109 14:28-40)).

Also, contrary to the district court’s assertion, the claims at issue in this case are similar to *Thales Visionix Inc. v. United States*. 850 F.3d 1343, 1348-49 (Fed. Cir. 2017) (rejecting lower court’s conclusion that the claims were merely directed to the abstract idea of using “mathematical equations for determining the relative position of a moving object to a moving reference frame” and instead finding the claims taught using inertial sensors in a non-conventional manner to reduce errors). Like in *Thales*, as detailed above, the methods and systems disclosed in the claims of Bytemark’s patents eliminate complications inherent in the previous mass transit ticketing methods and systems involving barcode scanners or paper tickets. Prior to the ‘967 patent, a barcode scanner was a necessary component in electronic ticket verification and authentication. The invention disclosed and claimed by Bytemark improved the electronic ticketing process by eliminating the need for a barcode reader or scanner through the use of a discrete and novel server-level token validation. *See, e.g.*, (Appx109 14:6-27) (“determining whether a token associated with the purchased electronic ticket has been stored in a data record associated with the received request, and if it has, whether the received token is valid”), (Appx137 14:12-28), (Appx103 1:28-43), (Appx112 1:31-46) (“Barcode scanners were not designed to read a lit LCD screen . . . [t]he reflectivity of the screen can defeat the scanning process.”)). As with the use of inertial sensors in a non-conventional manner in *Thales*, the Bytemark patents’ use of various known computer

components (e.g., servers and user computer devices such as mobile phones) in a non-conventional manner reduces errors associated with barcoding and improves the security and efficiency of server/computer/remote device communication to solve problems previously not addressed by the prior art. (Appx103 2:66-3:11, Appx103, Appx109-112, Appx137-138.)

Because the inventions disclosed and claimed in the ‘967 and ‘993 patents are not directed towards an abstract idea, the district court erred in finding the patents invalid as a matter of law, and the *Alice* inquiry should end at step one. *Enfish*, 822 F.3d at 1339.

2. The district court erroneously concluded that the asserted claims of the ‘967 and ‘993 patents lack an inventive concept.

In the event the Court finds that the ‘967 and ‘993 patents are directed toward an abstract idea, the claims of the patents contain an inventive concept under step two. In step two of the *Alice* analysis, the Court looks for “[a]n inventive concept that . . . is significantly more than the abstract idea itself, and cannot simply be an instruction to implement or apply the abstract idea on a computer.” *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016). A non-conventional and non-generic arrangement of known, conventional pieces can constitute an inventive concept. *Id.* at 1350; *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1302 (Fed. Cir. 2016). This Court has acknowledged

overlap between some step one and step two considerations, namely whether the claims teach an improvement over the prior art. *Ancora Techs.*, 908 F.3d at 1349.

In *Bascom*, this Court determined that the claims were directed to the abstract idea of “filtering content on the Internet.” *Bascom*, 827 F.3d at 1348. The *Bascom* court, however, held that the claims passed *Alice* step two because “[t]he inventive concept described and claimed in the ‘606 patent [was] *the installation of a filtering tool at a specific location, remote from the end users*, with customizable filtering features specific to each end user.” *Id.* at 1350 (emphasis added). In other words, the inventive concept was *where* monitoring took place within a network and *how* the monitoring was used (in a customizable way). Accordingly, the *Bascom* invention was not patent ineligible merely because it taught “monitoring” (an unconventional generic concept) generally.

Here, the claims of the ‘967 and ‘993 patents contain an inventive concept that solves technology related prior art problems. Prior to Bytemark’s claimed inventions, electronic ticketing methods and systems required the use of a barcode scanner for a venue to rely on to verify that a ticket is authentic and has not been pirated or tampered with. Bytemark also sought to address concerns with hacking visual validation display objects. (Appx132 4:41-47.) Bytemark’s claimed invention solves these problems. Specifically, claim 1 of the ‘967 patent overcame prior art problems with following inventive limitations: (i) receiving from the user's

computer device a token associated with the received request; (ii) determining whether a token associated with the purchased electronic ticket has been stored in a data record associated with the received request, *and if it has, whether the received token is valid*; and (iii) in dependence on the determination that the received token is valid, causing an activation of the purchased electronic ticket by transmitting to the user's computer device a data file comprising the visual validation display object that causes upon visual recognition by the ticket taker, the user to be permitted to utilize the service monitored by the ticket taker. (Appx109 14:14-27.)

As in *Bascom*, claim 1 of the '967 patent contains an inventive concept in how and when a token is used to overcome prior art electronic ticketing problems. For example, claim 1 conditions transmitting a data file comprising the visual validation display object on determining whether both (a) a token associated with the purchased ticket is stored in the data record; and (b) determining whether the received token is valid in such a way that a ticket taker does not need to rely on a barcode scanner for ticket verification. (Appx109 14:2-2, Appx103 1:40-43.)

Claim 1 of the '993 patent also does so by: *securing a validation display object prior to transmission* to provide a secured validation object; transmitting to the remote display device a secured validation display object associated; with the ticket payload; and enabling the remote display device to display the secured validation display object upon validation of the token for visual recognition by the ticket taker

or preventing the remote display device from displaying the secured validation display object in the event the token is not validated. (Appx137 14:13-34.)

By way of example, the specification of the '993 patent describes that the purpose of securing the visual validation display object prior to transmission is to solve prior art problems with tampering and piracy. (Appx132 3:12-23, Appx133 5:16-27.) The specification also describes *how* a visual validation display object can be secured. These examples include: securing the ticket payload code *in a region of the device* under the control of the telecommunications provider *so that the customer cannot access it* (Appx133 5:34-46); securing the visual validation display object by creating a kill parameter that destroys it upon expiration (Appx133 6:45-54); and packaging an animation for each device by the system server changing portions of the ticket payload so that the it is customized for each individual IMEI number associated with a ticket token and animation code comprising the ticket payload is designed so that it has to obtain the correct IMEI number at run time. (Appx133 5:47-67.)

Similar to *Bascom*, although Bytemark's inventions may use generic computer components, the inventions provide an inventive concept in using those components in an unconventional manner. Bytemark's inventions disclose a unique, ordered combination of how and when tokens and ticket payloads are transferred, how and when a visual display object is secured, and where on a device it is stored

(e.g., a location inaccessible to the user). Bytemark’s inventive, ordered combination of claim elements is necessary in overcoming the problems associated with prior art systems and methods.

Additionally, dependent claims 12 and 13 of the ‘993 patent disclose and claim the additional inventive limitation of displaying the secured visual validation display object without a connection with the central computer system, which Masabi’s own literature concedes is inventive. (Appx138 15:33-40.)

In its opinion, the district court failed to properly analyze whether the claims of the patents-in-suit include an inventive concept with respect to *Alice* step two. The district court’s two-paragraph opinion on this issue held that “in light of . . . step one . . . the asserted claims do not include an inventive concept,” and “the concept recited in the claims is nothing more than using . . . conventional tools to verify the authenticity of an electronic ticket.” (Appx3472-3473.) In so holding, the district court based its decision on hardware and software features in isolation and ignored addressing what the claims actually recite, contrary to the teachings of *Bascom*. See *Bascom*, 827 F.3d at 1348-50.

Arguments raised by Masabi in its Motion relating to step two of the *Alice* inquiry are also flawed and without merit. In its Motion, Masabi incorrectly argued that “Bytemark’s alleged improvements are not recited in the asserted claims or the asserted patents.” (Appx3222-3223.) Masabi also argued that there was no

inventive concept in the terms “token” and “securing” by assigning them unsupported simplistic definitions that are belied by the specification and in violation of how they should be read. (Appx3223-3225.) See *E.I. du Pont De Nemours & Co. v. Unifrax I LLC*, No. 2017-2575, 2019 WL 1646491, at *4 (Fed. Cir. Apr. 17, 2019) (“We cannot look at the ordinary meaning of [a] term . . . in a vacuum” but must consider “the context of the written description and the prosecution history.”).

Masabi’s argument that the claims of the patents-in-suit recite “fundamental tools and operation of the internet” such as “a server” and “a user’s computer device” and describe purely functional and generic steps is similarly without merit. Contrary to Masabi’s assertion, the claims of the ‘967 and ‘993 patents sufficiently disclose the validation and verification process through a specific implementation as the way in which the problems addressed by the specification are overcome by the patents.

Additionally, the cases that Masabi asserts are comparable are inapt. For example, in *Ultramercial, Inc. v. Hulu, LLC*, this Court held that “adding routine additional steps such as updating an activity log, requiring a request from the consumer to view the ad, restrictions on public access, and use of the Internet . . . comprises only conventional steps, specified at a high level of generality, which is insufficient to supply an inventive concept.” 772 F.3d 709, 716 (Fed. Cir. 2014). Other cases cited by Masabi similarly claim an abstract idea implemented on generic

computer components, without providing a specific technical solution beyond simply using generic computer concepts in a conventional way. *See Intellectual Ventures I*, 792 F.3d at 1371; *Content Extraction*, 776 F.3d at 1348; *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1344-45 (Fed. Cir. 2013).

In sum, even if the Court finds that the claims do not pass *Alice* step one, there are unconventional, non-routine, novel and inventive claim limitations disclosed in a specific combination that ensure that the asserted claims amount to significantly more than merely a patent on an abstract idea. As previously addressed, there are underlying factual issues of material fact with respect to some of these considerations, and the district court erred both in failing to consider these factual considerations and in finding the asserted claims ineligible as a matter of law.

CONCLUSION

For the foregoing reasons, the district court's decision should be reversed in its entirety.

Respectfully Submitted,

/s/ Dariush Keyhani
DARIUSH KEYHANI
KEYHANI LLC
1050 30th Street, NW
Washington, DC 20007
(202) 748-8950
dkeyhani@keyhanillc.com

ADDENDUM

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

BYTEMARK, INC.,

Plaintiff,

v.

MASABI LTD.,

Defendant.

§
§
§
§
§
§
§
§
§


Case No. 2:16-CV-00543-JRG-RSP

JUDGMENT

Before the Court is the Report & Recommendation [Dkt. No. 146] by Magistrate Judge Payne, which recommends that Defendant Masabi Ltd.'s Motion for Summary Judgment of Invalidity of U.S. Patent Nos. 8,494,967 and 9,239,993 [Dkt. No. 113] be granted under 35 U.S.C. § 101 and denied as moot as to Defendant's contentions of invalidity on other grounds. Having reviewed the matter *de novo* the Court concludes that Plaintiff's objections lack merit and Magistrate Judge Payne's Report & Recommendation is correct. Accordingly,

IT IS ORDERED AND ADJUDGED that Masabi Ltd.'s Motion for Summary Judgment of Invalidity of U.S. Patent Nos. 8,494,967 and 9,239,993 [Dkt. No. 113] is GRANTED under 35 U.S.C. § 101 and this action is DISMISSED WITH PREJUDICE.

So ORDERED and SIGNED this 7th day of February, 2019.



RODNEY GILSTRAP
UNITED STATES DISTRICT JUDGE



US008494967B2

(12) **United States Patent**
Bergdale et al.

(10) **Patent No.:** **US 8,494,967 B2**
(45) **Date of Patent:** **Jul. 23, 2013**

(54) **METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH VISUAL DISPLAY**

(75) Inventors: **Micah Bergdale**, New York, NY (US); **Matthew Grasser**, New York, NY (US); **Christopher Guess**, Brooklyn, NY (US); **Nicholas Ihm**, Brooklyn, NY (US); **Samuel Krueckeberg**, Brooklyn, NY (US); **Gregory Valyer**, Highland Park, IL (US)

(73) Assignee: **Bytemark, Inc.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **13/475,881**

(22) Filed: **May 18, 2012**

(65) **Prior Publication Data**

US 2012/0296828 A1 Nov. 22, 2012

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/110,709, filed on May 18, 2011, and a continuation-in-part of application No. 13/046,413, filed on Mar. 11, 2011.

(51) **Int. Cl.**
G06Q 20/00 (2006.01)

(52) **U.S. Cl.**
USPC **705/65**; 705/14.23; 705/14.25; 705/66; 705/67; 705/68; 705/69

(58) **Field of Classification Search**
USPC 705/14.23, 14.25, 65-69
See application file for complete search history.

(56) References Cited

U.S. PATENT DOCUMENTS

5,253,166 A *	10/1993	Dettelbach et al.	705/5
6,023,679 A *	2/2000	Acebo et al.	705/5
6,175,922 B1 *	1/2001	Wang	713/182
6,775,539 B2 *	8/2004	Deshpande	455/414.4
7,017,806 B2 *	3/2006	Peterson	235/384
7,134,087 B2 *	11/2006	Bushold et al.	715/764
7,158,939 B2 *	1/2007	Goldstein	705/5
7,191,221 B2 *	3/2007	Schatz et al.	709/206
7,386,517 B1 *	6/2008	Donner	705/75
7,493,261 B2 *	2/2009	Chen et al.	705/5
2001/0014870 A1 *	8/2001	Saito et al.	705/14
2002/0016929 A1 *	2/2002	Harashima et al.	713/201
2003/0036929 A1 *	2/2003	Vaughan et al.	705/5
2003/0105954 A1 *	6/2003	Immonen et al.	713/156
2003/0233276 A1 *	12/2003	Pearlman et al.	705/14
2004/0019564 A1 *	1/2004	Goldthwaite et al.	705/44
2004/0111373 A1 *	6/2004	Iga	705/51

(Continued)

FOREIGN PATENT DOCUMENTS

JP 11145952 * 5/1999
WO WO2007139348 A1 * 12/2007

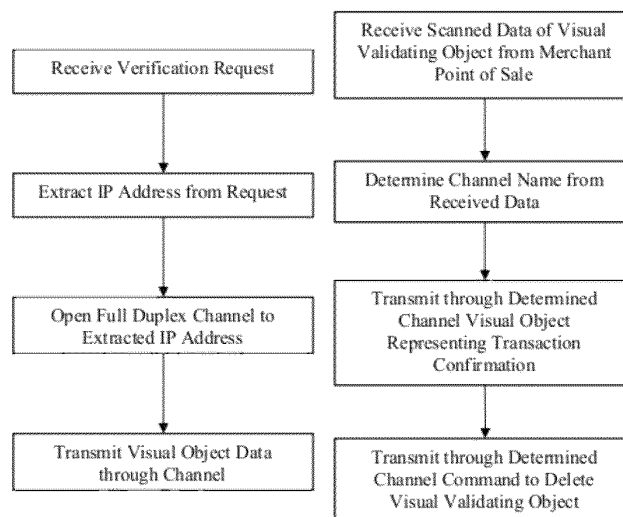
Primary Examiner — Calvin Cheung

(74) *Attorney, Agent, or Firm* — Ted Sabety, Esq.; Sabety & Associates, PLLC

(57) ABSTRACT

This invention discloses a novel system and method for distributing electronic ticketing such that the ticket is verified at the entrance to venues by means of an animation or other human perceptible verifying visual object that is selected by the venue for the specific event. This removes the need to use a bar-code scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders. The system providing the service also can maintain a persistent communication channel with the user device in order to control the ticket verification process.

34 Claims, 16 Drawing Sheets



US 8,494,967 B2

Page 2

U.S. PATENT DOCUMENTS

2004/0169589	A1 *	9/2004	Lea et al.	340/825.49	2007/0156443	A1 *	7/2007	Gurvey	705/1
2004/0186884	A1 *	9/2004	Dutordoir	709/206	2007/0271455	A1 *	11/2007	Nakano et al.	713/154
2004/0210476	A1 *	10/2004	Blair et al.	705/13	2008/0071587	A1 *	3/2008	Granucci et al.	705/5
2004/0224703	A1 *	11/2004	Takaki et al.	455/457	2008/0120127	A1 *	5/2008	Stoffelsma et al.	705/1
2005/0059339	A1 *	3/2005	Honda et al.	455/3.01	2008/0288302	A1 *	11/2008	Daouk et al.	705/5
2005/0272473	A1 *	12/2005	Sheena et al.	455/563	2008/0308638	A1 *	12/2008	Hussey	235/462.11
2006/0206724	A1 *	9/2006	Schaufele et al.	713/186	2010/0279610	A1 *	11/2010	Bjorhn et al.	455/41.2
2006/0293929	A1 *	12/2006	Wu et al.	705/5	2012/0166298	A1 *	6/2012	Smith et al.	705/24

* cited by examiner

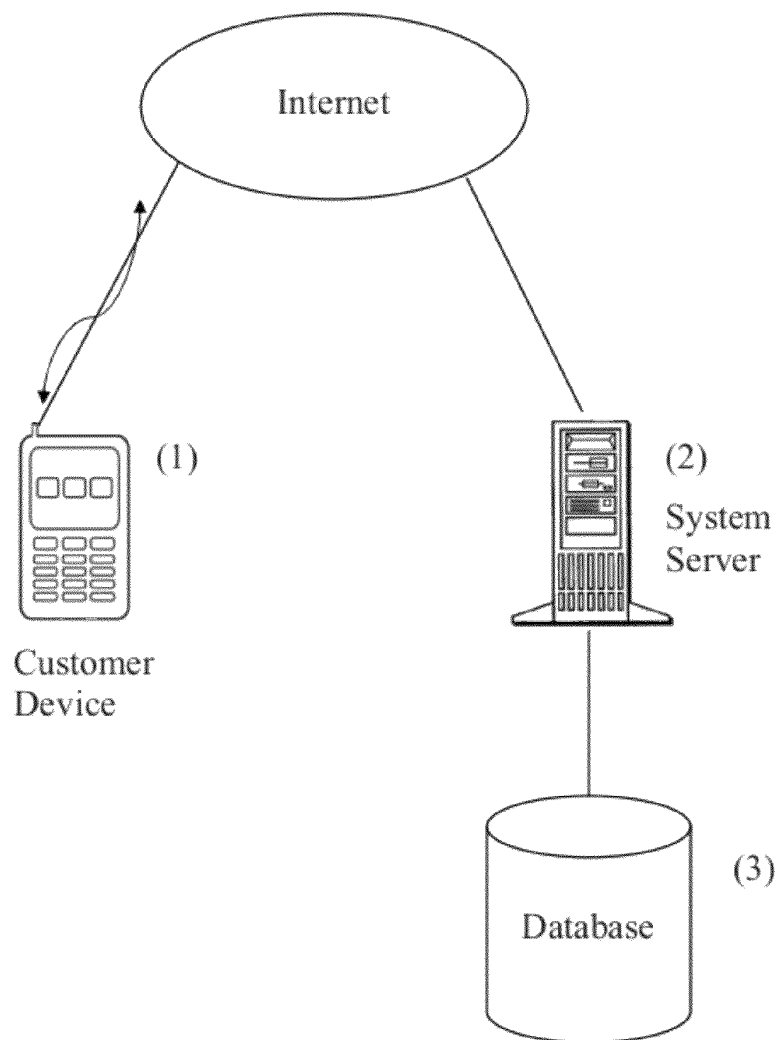
U.S. Patent

Jul. 23, 2013

Sheet 1 of 16

US 8,494,967 B2

Figure 1



U.S. Patent

Jul. 23, 2013

Sheet 2 of 16

US 8,494,967 B2

Figure 2

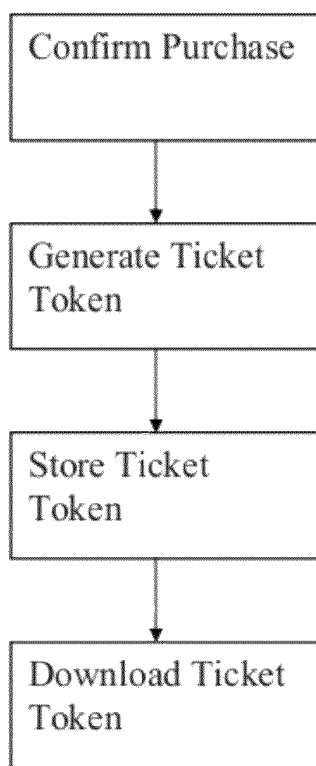
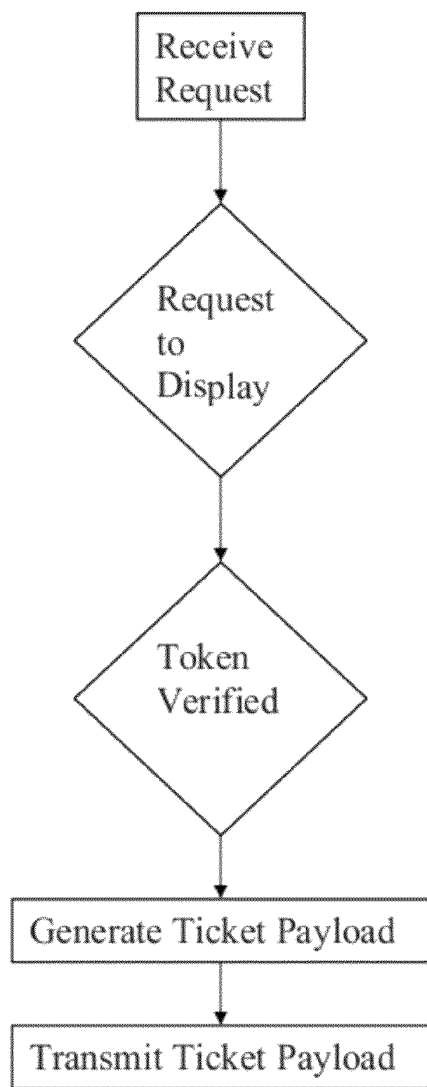


Figure 3



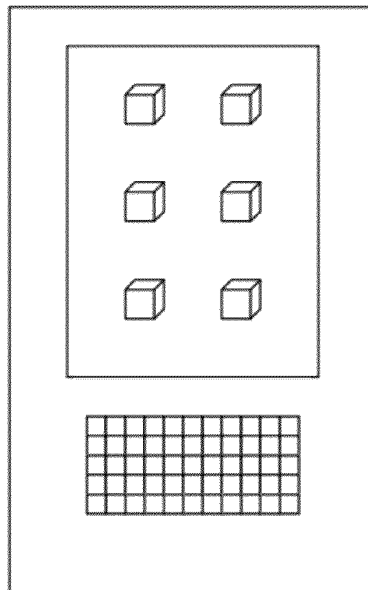
U.S. Patent

Jul. 23, 2013

Sheet 4 of 16

US 8,494,967 B2

Figure 4



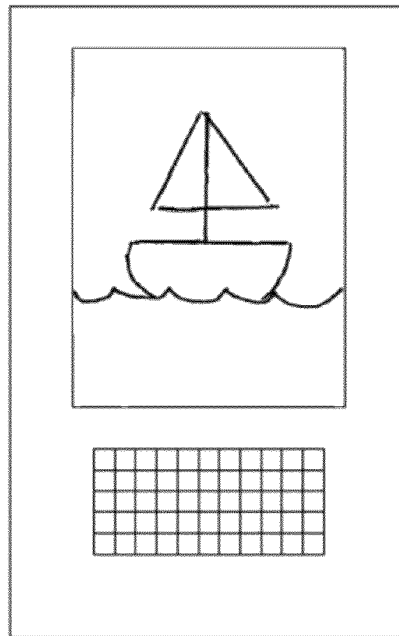
U.S. Patent

Jul. 23, 2013

Sheet 5 of 16

US 8,494,967 B2

Figure 5



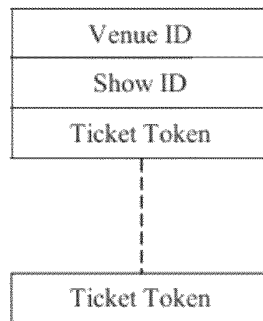
U.S. Patent

Jul. 23, 2013

Sheet 6 of 16

US 8,494,967 B2

Figure 6



U.S. Patent

Jul. 23, 2013

Sheet 7 of 16

US 8,494,967 B2

Figure 7

Venue ID
Username
Password

U.S. Patent

Jul. 23, 2013

Sheet 8 of 16

US 8,494,967 B2

P2P Buying & Selling

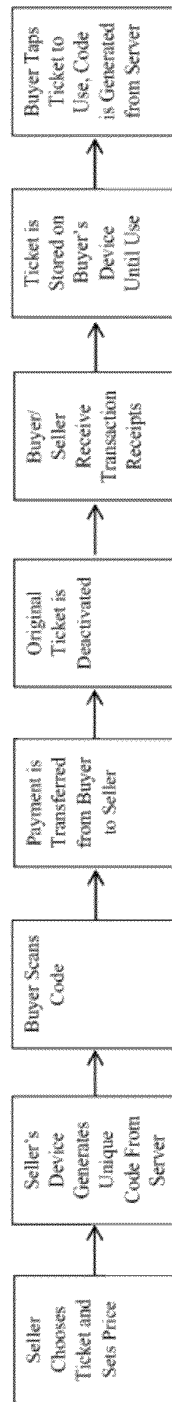


Figure 8

U.S. Patent

Jul. 23, 2013

Sheet 9 of 16

US 8,494,967 B2

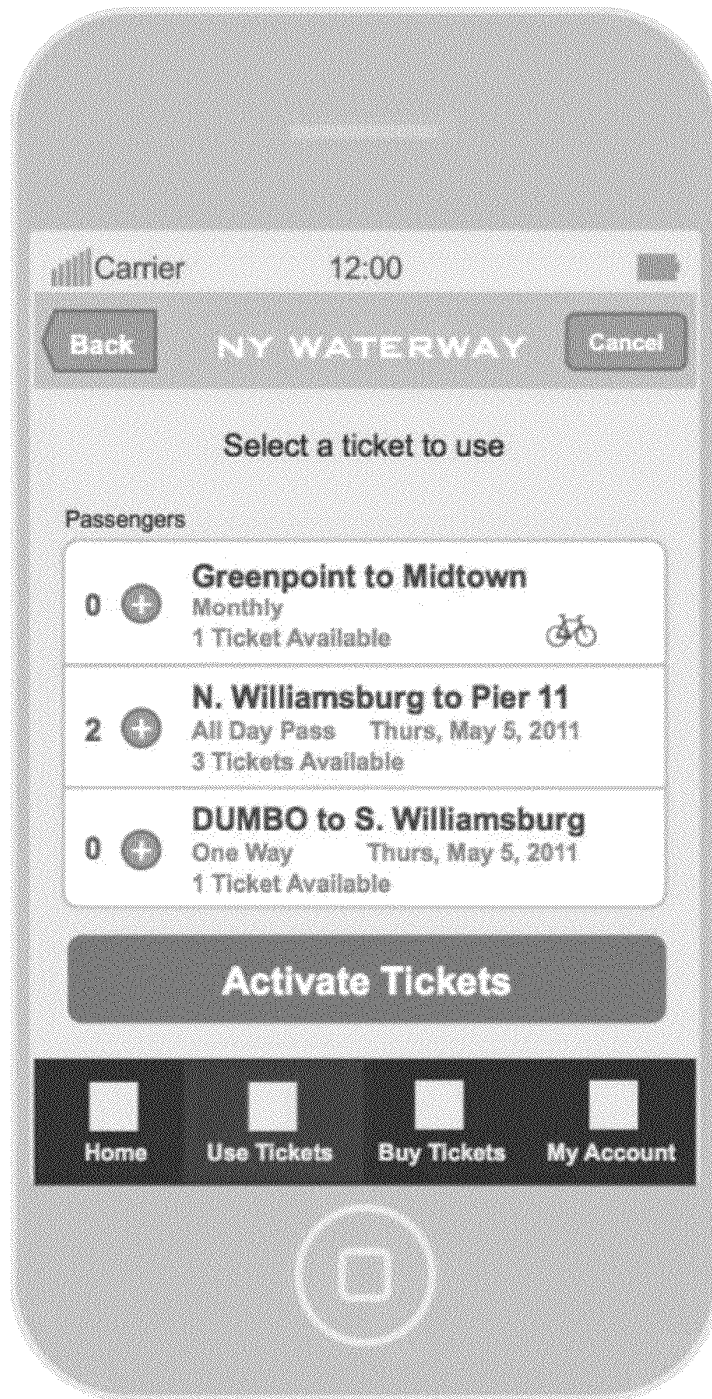


FIGURE 9

U.S. Patent

Jul. 23, 2013

Sheet 10 of 16

US 8,494,967 B2

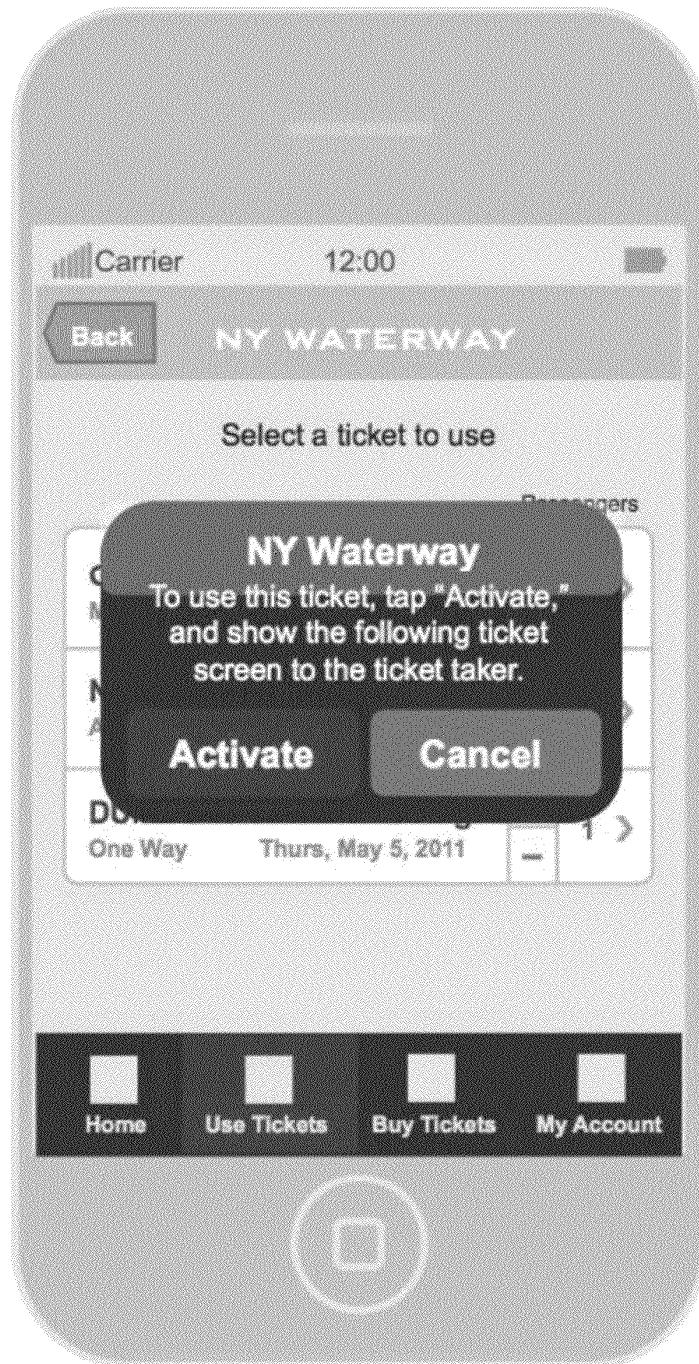


FIGURE 10

U.S. Patent

Jul. 23, 2013

Sheet 11 of 16

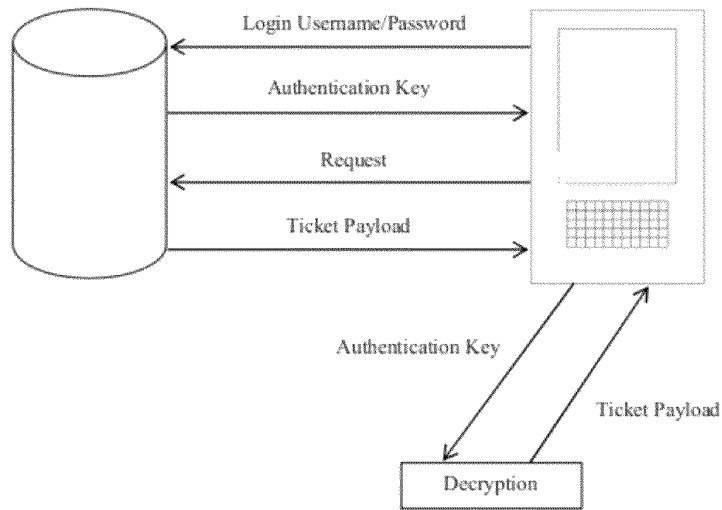
US 8,494,967 B2



FIGURE 11

Appx3299

Figure 12



U.S. Patent

Jul. 23, 2013

Sheet 13 of 16

US 8,494,967 B2

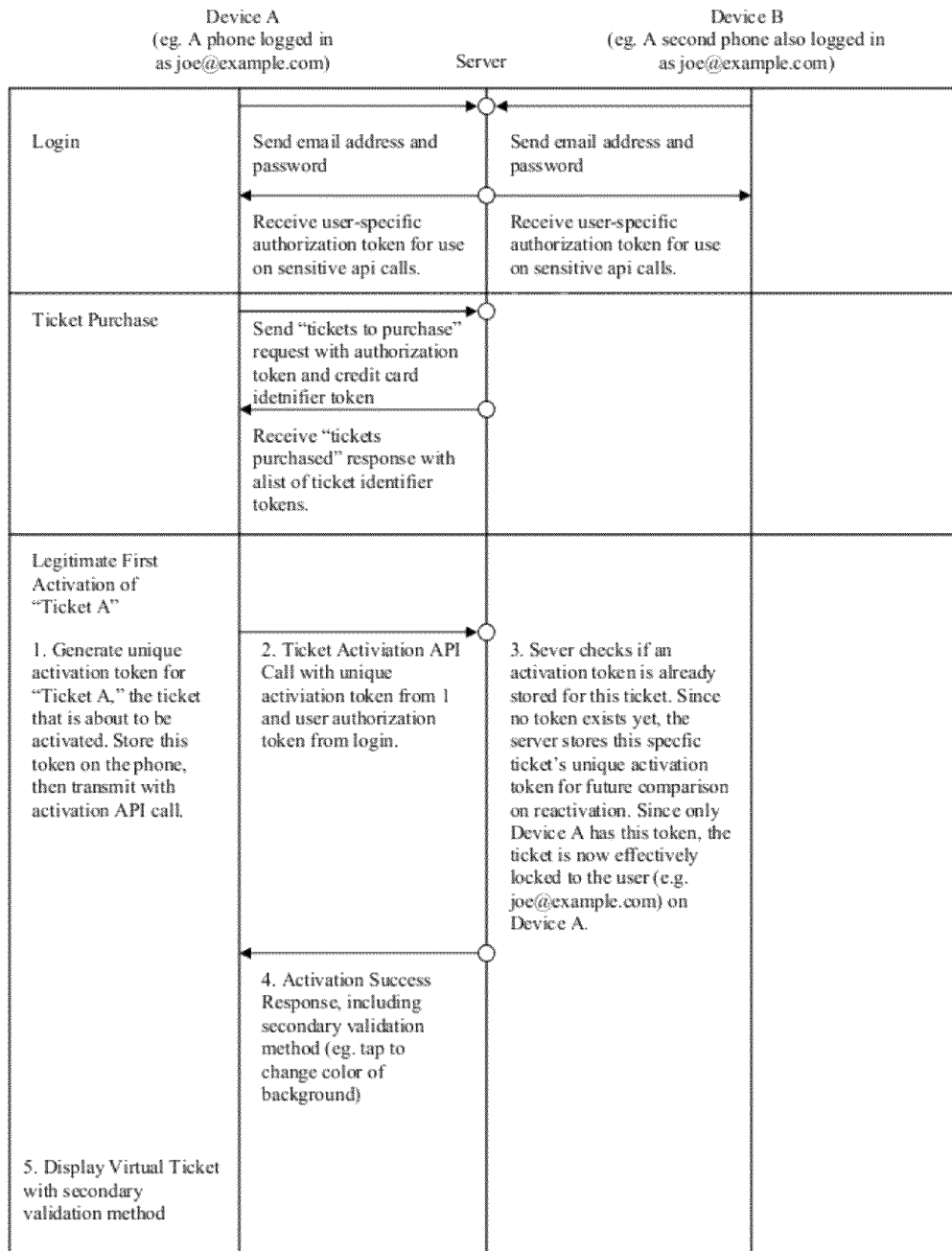


Fig. 13a

U.S. Patent

Jul. 23, 2013

Sheet 14 of 16

US 8,494,967 B2

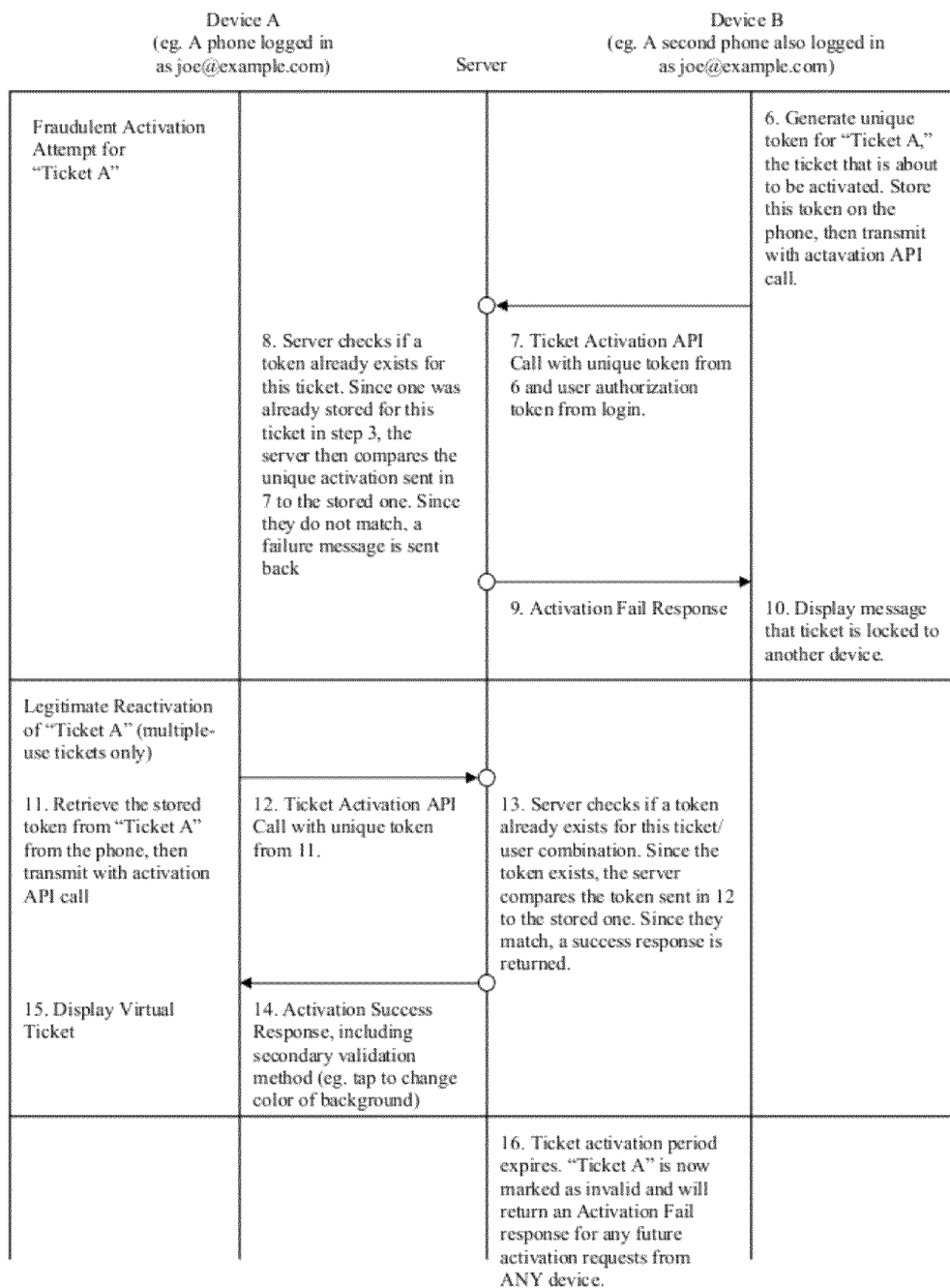


Fig. 13b

U.S. Patent

Jul. 23, 2013

Sheet 15 of 16

US 8,494,967 B2

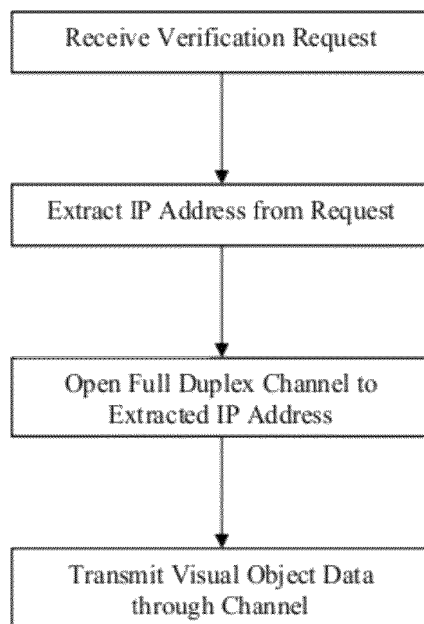


Fig. 14

Appx3303

U.S. Patent

Jul. 23, 2013

Sheet 16 of 16

US 8,494,967 B2

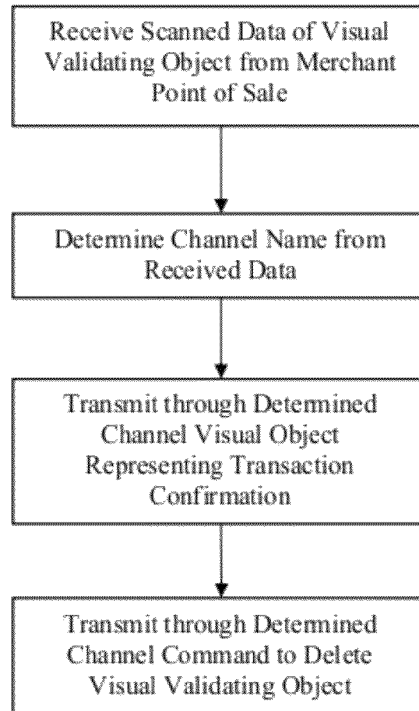


Fig. 15

US 8,494,967 B2

1

METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH VISUAL DISPLAY

This patent application claims priority to U.S. patent application Ser. No. 13/110,709 filed on May 18, 2011 as a Continuation in Part and hereby incorporates that application by reference in its entirety. This application also claims priority to U.S. patent application Ser. No. 13/046,413 filed on Mar. 11, 2011 as a Continuation in Part and hereby incorporates that application by reference in its entirety.

FIELD OF INVENTION

This invention provides a mechanism whereby a venue or other facility that meters usage by means of tickets can distribute tickets electronically and use a visual aid on an electronic device to visually confirm that a person is a valid ticket holder.

BACKGROUND

Venues such as theaters, amusement parks and other facilities that use tickets, for example airlines, ferries and other transportation have a need to use electronic ticketing. Existing systems distribute information that can constitute a ticket, but the verification problem is difficult. In one example of prior art, an electronic ticket is displayed as a bar-code on the recipient's telephone display screen. The telephone is then placed on a scanner that reads the bar-code in order to verify the ticket. The problem with these systems is that the scanning process is fraught with error and the time taken to verify the electronic ticket far exceeds that of the old system: looking at the paper ticket and tearing it in half. Barcode scanners were not designed to read a lit LCD screen displaying a bar code. The reflectivity of the screen can defeat the scanning process. Therefore, there is a need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket. This invention provides for the distribution of an electronic ticket that also contains a visual display that ticket takers can rely on as verification, without using a scanning device.

DESCRIPTION OF THE FIGURES

- FIG. 1. Basic architecture.
- FIG. 2. Flow chart for ticket purchase.
- FIG. 3. Flow chart for displaying the verifying visual object.
- FIG. 4. Example validating visual object.
- FIG. 5. Example validating visual object
- FIG. 6. Schematic of event database record.
- FIG. 7. Schematic of authorized user database record.
- FIG. 8. Flow chart for transfer of ticket.
- FIG. 9. Example user interface on user's device.
- FIG. 10. Example user interface showing activation selection screen.
- FIG. 11. Example user interface showing display of validating visual object and other ticketing information.
- FIG. 12. Flowchart for ticket activation process.
- FIG. 13a. Protocol diagram for activation process.
- FIG. 13b. Continued protocol diagram for activation process.
- FIG. 14. Flowchart for persistent channel.
- FIG. 15. Flowchart for persistent channel for purchase verification.

2

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The system operates on one or more computers, typically one or more file servers connected to the Internet and also on a customer's computing device. A customer's device can be a personal computer, mobile phone, mobile handheld device like a Blackberry™ or iPhone™ or any other kind of computing device a user can use to send and receive data messages. The customer's device is used to display the validating visual object.

Conventional electronic tickets display a barcode or QR code on a user's telephone, typically a cellphone or other portable wireless device with a display screen. The problem with this approach is that a barcode scanner has to be used by the ticket taker. Barcode scanners are not highly compatible with LCD screen displays of barcodes. The amount of time that it takes to process an electronic ticket is greater than that of a paper ticket. Sometimes the LCD display does not scan at all and a passenger has to be sent away to get a paper printout of a ticket. Given the potential large crowds that often attend open venues, this is impractical.

In this invention, the ticket is procured electronically and stored on the user's device. However, when the ticket is to be taken the verification is determined by a larger visual object that a human can perceive without a machine scanning it. The particular validating visual object chosen can be constantly changed so that the ticket taker does not have to be concerned that a device displaying the designated validating visual object is invalid. There are many types of visual objects that can be displayed that are easily recognized by a ticket taker. These can include but are not limited to: Patterns of color change, Animations and Geometric patterns. In one embodiment, the validating visual object that is transmitted can be computer code, that when executed by the device, causes the user device to display the desired visual pattern. In another embodiment, the validating visual object is a command that specifies what the visual pattern should be. In that embodiment, the program operating on the user's device receives the command instruction, decodes it, and determines what visual patterns to generate based on the data in the command instruction. In another embodiment, the validating visual object is video or image data transmitted directly from the server to the device for immediate display.

In one embodiment of the invention, the user purchases a ticket from an on-line website. The website sends to the user's device a unique number, referred to as a token. The token is also stored in the ticketing database. When the time comes to present the ticket, the venue can select what visual indicator will be used as the designated validation visual object. The user can then request the validation visual object. The user's device will have an application that launches a user interface. The user can select "validate" or some other equivalent command to cause the application to fetch and download from the ticketing system a data object referred to herein as a ticket payload, which includes a program to run on the user's device. In another embodiment, the ticket payload can be pushed to the device by the venue. As a result, the application transmitted to the user's device is previously unknown to the user and not resident in the user's device. At that point the user's device can execute the program embodied in the ticket payload, which causes the validation visual object to be displayed on the user's device. The ticket taker knows what the validating visual object is, and simply looks to see that the user's device is displaying the correct visual object.

Piracy is limited in several ways. First, the ticket holder and their device does not have access to the validating visual

US 8,494,967 B2

3

object until a time select to be close to the point in time where the ticket has to be presented. Second, the validating visual object is one of an very large number of permutations and therefore cannot be guessed, selected or copied ahead of time. Third, the ticket payload can contain code that destroys the validating visual object in a pre-determined period of time after initial display or upon some pre-determined input event. Fourth, a number of security protocols can be utilized to ensure that a copy of the application that executes to display the validating visual object cannot be readily copied or reverse engineered.

Validating Visual Object Displays:

There many kinds of validation displays that can be utilized. The criterion for what constitutes a validating visual object is one that is readily recognizable from human observation, is encapsulated in such a way as to be transmitted to the customer's device with a minimum of network latency or download time, and that can be reasonably secured so as to avoid piracy.

Barcodes and similar codes like the QR code are not validating visual objects because a person looking at them cannot tell one apart from another. Instead, the person has to rely on a barcode scanner and computing device to verify the barcode.

In one embodiment, the period that a particular validating visual object may be used is automatically limited. Examples of validating visual objects include:

1. A color display on the device.
2. A color sequence.
3. An animation that is easily recognized.
4. Animations can include easily recognizable geometric patterns, for example an array of diamonds, or an array of rotating cubes.
5. A human recognizable image.
6. The customer's face as an image.
7. Combinations of the above.

In another embodiment, other images, for example, block letter, can be displayed so that additional information readily apparent to the ticket taker is displayed. For example, a letter can be designated for a Child ticket or a different letter for an Adult ticket.

Referring now to FIG. 1, the customer uses their device (1) to purchase a ticket from the service operating the system server (2) and database (3).

In one embodiment, an authorized user associated with the venue, typically the box office manager, logs into the back-end system through a secure web-page. The authorized user can enter the web-page by entering a username, password and venue identifier. The system maintains a database (3) that associates the venue identifier with a set of usernames and password pairs that are authorized to use the system on behalf of the venue. See FIG. 7. The system checks the database (3) to verify that the venue ID, username and password are consistent with each other. The authorized user can navigate through to a point in the system user interface where a particular show may be selected for ticket taking. The user selects the upcoming show, and then selects from a display of possible validating visual objects. The validating visual object is transmitted to a device viewable by ticket taking staff at the entrances to the venue. The staff then can see the authorized object to accept for the upcoming show.

Ticket holders that have purchased tickets have a data record in the system database that contains the unique token associated with the ticket and other relevant information, including the venueID and an identifier identifying the specific show the ticket is for. See FIG. 6. At the entrance, customers are requested to operate an application on their devices. This application fetches the stored ticket token and

4

transmits that token to the system, preferably over a secure data channel. The database looks up the token to check that the token is valid for the upcoming show. If the token is valid, then the system transmits back to the device a ticket payload. The ticket payload contains computer code that, when operated, displays the selected validating visual object.

The customer can navigate the user interface of the application in order to cause the application to request whether to display the validating visual object. As shown in FIG. 9, one or more available tickets can be displayed on the user interface, which provides the user the ability to select one of the tickets. When the customer properly actuates the user interface, for example, by actuating the "Activate Tickets" button (see FIG. 10), the validating visual object is displayed on the screen of the device. The animation can be presented along with other ticketing information (see FIG. 11). In one embodiment, the device transmits the ticket token to the system with a command indicating that the ticket has been used. In another embodiment, the customer can operate the application and request that the application transmit to the database the condition that the ticket was used. In that embodiment, the user can input a numeric code or password that the application uses to verify that the customer is confirming use of the ticket. In yet another embodiment, after the validating visual object has been launched, a predetermined amount of time later it can be deemed used. At that time, the application can cause the color of the object to be changed so that it indicates that there was a valid ticket, but the ticket was used. This condition is useful in cases where the venue checks tickets during shows while letting customers move around the venue's facilities.

In another embodiment, the purchase of the ticket causes the ticket payload to be downloaded to the customer's device. Likewise, the authorized user for the venue will select a validating visual object for a particular show well in advance of the show. In this case, because a customer may possess the payload some time before its use, precautions must be taken to secure the ticket payload from being hacked so that any similar device can display the validating visual object. While this is a security tradeoff, the benefit is that the customer need not have an Internet connection at a time close to the show-time of the venue.

The use of electronic ticketing provides opportunities that change how tickets can be bought and sold. For example a first customer can purchase a ticket and receive on their device a ticket token. A second customer can purchase that ticket using the system. The first customer can use the application to send a message to the system server indicating that the first customer intends to the web-page indicating that it wants to buy that particular ticket. The system can ask the first customer for a username and password to be associated with the first customer's ticket. If the second customer identifies the first customer's username, the system then can match the two together. At that point, the data record associated with the first customer's ticket is modified so that the ticket token value is changed to a new value. That new ticket token value is then transmitted to the second customer's device. At the same time, the system can operate a typical on-line payment and credit system that secures payment from the second customer and credits the first customer. In one embodiment, the system pays the first customer a discounted amount, retaining the balance as a fee.

In yet another embodiment, the first customer may be unknown to the second customer. In that embodiment, the first customer simply may indicate to the system, through a message transmitted from the application operating on the device or directly through a web-page, that the first customer

US 8,494,967 B2

5

is not going to use the ticket and wishes to sell it. At that point, the system can mark the data record associated with the ticket as "available for sale." When the second customer makes a request to purchase a ticket for the same show, the system creates a new ticket token for the second customer and updates the ticket token stored in the data record.

In a general admission type of scenario, the ticketing database is simple: each show has a venue ID, some identifier associated with the show itself, various time indicators, the selected validating visual object, and a list of valid ticket tokens. In a reserved seating arrangement, the ticketing database has a data record associated with a show, as indicated by a show identifier, but each seat has a data record that has a unique show identifier and ticket token, which includes the identity of the seat itself.

In the preferred embodiment, the validating visual object is secured against tampering. One threat model is that a customer who has received a ticket payload would then take the data file comprising the ticket payload and analyze it to detect the actual program code that when executed, produces the validating visual object on the display screen of the device. Once that has been accomplished, the would-be pirate can then re-package the code without any security mechanism and readily distribute it to other device owners, or even cross-compile it to execute on other types of display devices. The preferred embodiment addresses this threat model in a number of ways.

First, the ticket payload can be secured in a region of the device under the control of the telecommunications provider. In this case, the customer cannot access the code comprising the ticket payload. In another embodiment, the ticket payload can be encrypted in such a way that the only decrypting key available is in the secure portion of the telecommunications device. In that embodiment, the key is only delivered when an application running on the secure part of the device confirms that the ticket payload that is executing has not been tampered with, for example, by checking the checksum of its run-time image. At that point, the key can be delivered to the ticket payload process so that the validating visual object is displayed on the device.

Second, the selected animation is packaged for each device. That is, the code that operates to display the validating visual object itself operates certain security protocols. The phone transmits a ticket transaction request. The request includes a numeric value unique to the device, for example, an IMEI number. Other embodiments use the UDID or hardware serial number of the device instead of or in combination with the IMEI number. The system server then generates the ticket token using the IMEI number and transmits that value to that device. In addition, the ticket payload is created such that it expects to read the correct IMEI number. This is accomplished by the system server changing portions of the ticket payload so that the it is customized for each individual IMEI number associated with a ticket token. The animation code comprising the ticket payload is designed so that it has to obtain the correct IMEI number at run time. In another embodiment, at run-time, the animation code will read the particular ticket token specific for the phone that instance of the animation was transmitted to. The code will then decode the token and check that it reflects the correct IMEI number for that device.

In another embodiment, the security protocol first requires the user to login to the server with a login username and password. The application also transmits the IMEI, UDID or serial number of the device or any combination of them. When verified by the server, an authorization key (Authkey) is transmitted to the device. The Authkey is a random number.

6

When the user's application transmits a request for a validating visual object, it transmits the Authkey and the IMEI, UDID or serial number (or combination) that is used for verification. This is checked by the server for validity in the database. On verification, the validating visual object is encrypted using the Authkey and transmitted to the device. The application running on the device then uses the Authkey to decrypt and display the validating visual object. The Authkey is a one-time key. It is used once for each ticket payload. If a user buys a second ticket from the system, a different, second Authkey is associated with that second ticket payload. In one embodiment, the Authkey is unique to the ticket for a given event. In another embodiment, the Authkey is unique to the ticket, device and the event. In other embodiments, the Authkey can be replaced with a key-pair in an asymmetric encryption system. In that case, the validating visual object is encrypted with a "public" key, and then each user is issued a private key as the "Authkey" to be used to decrypt the object.

In yet another embodiment, the Authkey can be encrypted on the server and transmitted to the device in encrypted form. Only when the application is operating can the Authkey be decrypted with the appropriate key. In yet another embodiment, the application that displays the validating visual object can request a PIN number or some other login password from the user, such that if the device is lost, the tickets cannot be used by someone who finds the device.

In another embodiment, the application running on the device can fetch a dynamic script, meaning a piece of code that has instructions arranged in a different order for subsets of devices that request it. The ticket payload is then modified so as to have the same number of versions that are compatible with a corresponding variation in the dynamic script. As a result, it is difficult to reverse engineer the application because the application will be altered at run time and the ticket payload customized for that alteration. One embodiment of the dynamic script would be expressed in Java™ computer language and rendered using OpenView. The ticket payload can be an HTML file called using Ajax.

Security can also be enhanced by actively destroying the validating visual object so that it resides in the device for a limited time. In one embodiment, the ticket payload has a time to kill parameter that provides the application with a count-down time to destroy the validating visual object. In another embodiment, the validating visual object is displayed when the user holds down a literal or virtual button on the user interface of the device. When the button is released, the application destroys the validating visual object.

Security can also be enhanced by retaining as steganographic data embedded in the validating visual object, the IMEI, UDID, Serial number or phone number of the device. The application can be operated to recover that information and display it on the screen. This makes it possible for security personnel at a venue to view that information from a validly operating device. If the device is showing a pirated validating visual object, then the actual data associated with the device will not match and it will be apparent from inspection of the device. This way, suspicious ticket holders can be subject to increased scrutiny, the presence of which deters piracy.

In another embodiment, the ticket payload can operate a sound sampling application that requests the customer to speak in to the device. The application can then use that data to check whether the voice print of the speaker matches the expected voice print. In yet another embodiment, the device can take a picture of the customer's face, and then facial recognition code embedded in the ticket payload can operate to check whether the features of the face sufficiently match a

US 8,494,967 B2

7

pre-determined set of features, that is, of the customer's face at the time the ticket was purchased. In yet another embodiment, the verification can be supplemented by being sure that the use of the ticket is during a pre-determined period of time. In yet another embodiment, the verification can be supplemented by the ticket payload operating to check that the location of the venue where the ticket is being used is within a pre-determined range of tolerance to a GPS (Global Positioning System) location. In yet another embodiment, after a certain pre-determined number of downloads of ticket payloads for a specific show, the validating visual object is automatically changed. This last mechanism may be used for promotions, to select the first set of ticket buyers for special treatment at the venue. In yet another embodiment, two different validating visual objects may be used, which are selected based on the verified age of the customer. In this way, a venue can use the system to not only to verify ticket holders coming into the venue, but to verify their drinking age when alcoholic drinks are ordered.

In yet another embodiment, the system's servers control the ticket activation process. FIG. 12. In this embodiment, the token is generated randomly by the user's mobile computing device and then transmitted to and stored on the system server as a result of the user's request to activate the ticket. When the server receives a request to activate a ticket, the server checks whether there is already an activation token stored in its database that corresponds to that ticket. The token is stored in a data record associated with the user that is activating the ticket. The user logs into the account and then requests that a ticket be activated. If it is, then it checks whether the token received from the user's mobile device matches the stored token. That is, it authenticates against that stored token. If the user's request for activation is the first activation of the ticket, then the server stores the received token into the data record associated with the user's account and keeps it there for a predetermined period of time, in order to lock the ticket to that device for that period of time. This process locks a ticket to that unique token for that lock period. Typically this will lock the ticket to the user's mobile computing device. If the stored token does not match the token received from the user's computing device, the ticket activation is denied.

The predetermined lock time permits a reusable ticket to be locked to a device for the predetermined lock time. This is useful in the event the user changes the mobile computing device that the user uses to the ticket. For example, a monthly train commuting ticket would be activated once each day, and would remain activated for the day of its activation. In this case, the user would validate the ticket once each day, and that activation would be locked to the device for the day. The next day, the user would be able to activate the ticket using a different mobile computing device if the predetermined time locking the activation has expired, that is, if the data record associated with the ticket has been automatically reset into an deactivated state. The activation process also permits a user account to be shared within a family, for instance, but that each ticket sold to that account to be locked to one device.

As depicted in the protocol diagrams FIGS. 13a and 13b, the user can use their mobile computing device to request that their ticket get activated for the first time. However, once that activation process has occurred, the server will store the unique token received from the activating user's computing device in the database in a manner that associates it with the ticket and the user's account. If another user associated with the account attempts to use the ticket by activating it, a different random token will be transmitted to the server. Because these two tokens do not match, the second activation will be prohibited.

8

The activation process can also permit a ticket to be shared. In this embodiment, the user who has activated the ticket can submit to the server a request that the ticket be transferred to another user. For example, a data message can be transmitted from the user's device to the system that embodies a request to move the ticket to another user. In that case, the stored token is marked as blocked, or is equivalently considered not present. This is accomplished by storing a data flag in the database that corresponds to the ticket. One logic state encodes normal use and the opposite logic state encodes that the ticket has been shared. A data message may be transmitted to the second user indicating that the ticket is available for activation. The second user may submit a request to activate the ticket and a random token value is transmitted from the second user's device to the server. That second token value is checked to see if it's the first activation. Because the first user has activated the ticket, but then transferred it, the activation by the second user is not blocked. That is, the server detects that the first token is now cancelled or equivalently, the system has returned to the state where the first activation has not occurred and therefore permits the new activation to take place. The new activation can also have a predetermined time to live value stored in the database that is associated with it. In this case, the activation by the second user expires and the second user can be prevented from reactivating the ticket. At the same time, the flag setting that disables the first token can be reset, thereby setting the ticket up for reactivation by the first user. By this mechanism, it is possible for the electronic ticket to be lent from one user to another.

In yet another embodiment, the ticket activation process can open a persistent connection channel over the data network that links the server and the user's mobile computing device. In this embodiment, if the activation of the ticket and therefore the device is successful, the server can maintain a persistent data channel with a computer process running on the user's computing device. In this embodiment, the request for ticket activation causes the user computer device to open the persistent channel. In this embodiment, the server establishes a communication process operating on the server that receives data and then causes that data to be automatically routed to the user's computing device. The process on the user's mobile computing device can thereby automatically respond to that received data. In tandem, the computer process operating on the users computing device can send data directly to the server process associated with that user's session. For a server servicing many user devices, there will be one persistent channel established between the server and each mobile device that has an activated ticket.

The persistent channel between the server and the user's computer device can be used in a variety of ways. In the preferred embodiment, the persistent connection is designed so that that it maintains a bi-directional, full-duplex communications channel over a single TCP connection. The protocol provides a standardized way for the server to send content to the process operating on the user's computing device without being solicited by the user's device each time for that information, and allowing for messages to be passed back and forth while keeping the connection open. In this way a two-way (bi-direction) ongoing interaction can take place between a process operating on the user's computing device the server. By means of the persistent channel, the server can control the activity of the user computer device. For each user computing device, there can be a distinct persistent connection.

In one embodiment, the persistent connection is established when the user requests an activation of a ticket. See FIG. 14. In other embodiments, it can be used if the system is

US 8,494,967 B2

9

used to verify payment of a purchase price. In either case, the user computing device transmits a request message to the server. For each user computing device, there can be a distinct persistent channel. Each persistent channel has a label or channel name that can be used by the server to address the channel. In the case of ticketing, when the ticket is activated the data representing the validating visual object can be transmitted in real time from the server to the user computing device and immediately displayed on the device. This provides an additional method of securing the visual ticketing process. In this case, when the ticket is activated and the persistent channel is created, the label of the channel is stored in the database in a data record associated with the user and the ticket. When the server transmits the validating visual object for that ticket, it fetches from the database the label of the channel and then uses that label to route the transmission of the validating visual object. The use of the persistent channel causes the user computer device to immediately and automatically act on the validating visual object. In one embodiment, the receipt of the validating visual object causes the receiving process to immediately in response interpret the command and select and display the required visual pattern. In another embodiment, the process receives a block of code that the process calls on to execute, and that code causes the visual pattern to be displayed. In yet another embodiment, the process receives image or video data and the process passes that data on to the user device screen display functions for presentation on the user device screen.

In another embodiment, a validating visual object can be transmitted to the user's computing device to be automatically displayed on the screen without the user having to input a command to cause the display. That visual object can be displayed by the user computing device. For additional security, the server can transmit to the user computing device a visual object that contains the channel name or a unique number that the server can map to the channel name. For clarity, this additional visual object is not necessarily used for visual verification by ticket takers, as explained above. This visual object can be used by other machinery to confirm the ticket purchase transaction or even other transactions not directly related to the purchase of the ticket. The additional visual object can be in the form of a QR code, barcode or any other visual object that can be scanned, for example at a point of sale system, and from that scanned image, an embedded data payload extracted. In that visual object, data can be embedded that uniquely identifies the source of the scanned object. The channel name of the persistent channel or a number uniquely mapped on the server to identify the channel can be embedded in that scanned object.

In one embodiment, as shown on FIG. 15, a merchant can use a point of sale system operated by the merchant to scan the display screen of the user's computing device. That point of sale system can then capture from the scanned image the channel name or a unique number that is uniquely mapped on the server to the channel name. That information is transmitted to the server as a challenge for verification. The received challenge data is checked to see if it matches the channel name or corresponding unique number used to transmit the visual object that the merchant scanned. If they match up, there is a verification of a transaction. This exchange provides verification that the user's device is present at the merchant location and that a transaction with the merchant should be paid for.

In yet another embodiment, the persistent connection provides a means for the server to control the actions of the process operating on the user's computer device that is at the other end of the connection. In this embodiment, the server

10

can automatically transmit a command to the process on the user's computing device that automatically deletes the verifying visual object that has been transmitted to ensure that it cannot be reused or copied.

In one embodiment, the persistent connection is used to automatically transmit visual information to the user's mobile computing device and to cause that information to be displayed on the screen of the device. The visual information can be the validating visual object or any other visual object that the server selects to transmit for display. In this embodiment, the persistent connection can be used by the server to transmit other information to the user's device. In this embodiment, the server transmits text, images, video or sound and in some cases in combination with other HTML data. In another embodiment, this material comprises advertising that the server selects to display on the user's device. The selection process can utilize the GPS feature described above to determine the approximate location of the user's device and then based on that location, select advertising appropriate to be transmitted to that device. In yet another embodiment, the server selects the advertising content by determining predetermined features of the validated ticket or purchasing transaction and then making a selection on the basis of those features. For example, a validation of a ticket to a baseball game played by a team specified in the data associated with the validated ticket may cause the selection of an offer to purchase a ticket for the next baseball game of the same team. In yet another embodiment, the character of the transaction being verified can be used to cause the selection of advertising or the transmission of data comprising a discount offer related to the transaction.

In this embodiment, the server receives from the merchant the data that determines the persistent channel. The merchant, by relying on the system for payment will also transmit transaction details, for example, an amount of money and an identity of goods or services. When the channel name or unique number associated with the channel is matched for verification, the server can transmit data representing a confirmation display down to the user's device using the persistent connection. This data is received by the user computing device and then automatically rendered by the process at the other end of the channel connection. In addition, the server can use the transaction information to determine one or more advertisements or discount offers to transmit to the user's computing device. The selection method can consist of one or more heuristics. In one example, the validation of the ticket for a baseball game can trigger the display of advertising for food or drinks. Likewise, a transaction for purchasing a cup of coffee can trigger an advertisement for purchasing a newspaper.

Operating Environment:

The system operates on one or more computers, typically one or more file servers connected to the Internet. The system is typically comprised of a central server that is connected by a data network to a user's computer. The central server may be comprised of one or more computers connected to one or more mass storage devices. A website is a central server that is connected to the Internet. The typical website has one or more files, referred to as web-pages, that are transmitted to a user's computer so that the user's computer displays an interface in dependence on the contents of the web-page file. The web-page file can contain HTML or other data that is rendered by a program operating on the user's computer. That program, referred to as a browser, permits the user to actuate virtual buttons or controls that are displayed by the browser and to input alphanumeric data. The browser operating on the user's computer then transmits values associated with the

US 8,494,967 B2

11

buttons or other controls and any input alphanumeric strings to the website. The website then processes these inputs, in some cases transmitting back to the user's computer additional data that is displayed by the browser. The precise architecture of the central server does not limit the claimed invention. In addition, the data network may operate with several levels, such that the user's computer is connected through a fire wall to one server, which routes communications to another server that executes the disclosed methods. The precise details of the data network architecture does not limit the claimed invention. Further, the user's computer may be a laptop or desktop type of personal computer. It can also be a cell phone, smart phone or other handheld device. The precise form factor of the user's computer does not limit the claimed invention. In one embodiment, the user's computer is omitted, and instead a separate computing functionality provided that works with the central server. This may be housed in the central server or operatively connected to it. In this case, an operator can take a telephone call from a customer and input into the computing system the customer's data in accordance with the disclosed method. Further, the customer may receive from and transmit data to the central server by means of the Internet, whereby the customer accesses an account using an Internet web-browser and browser displays an interactive webpage operatively connected to the central server. The central server transmits and receives data in response to data and commands transmitted from the browser in response to the customer's actuation of the browser user interface.

A server may be a computer comprised of a central processing unit with a mass storage device and a network connection. In addition a server can include multiple of such computers connected together with a data network or other data transfer connection, or, multiple computers on a network with network accessed storage, in a manner that provides such functionality as a group. Practitioners of ordinary skill will recognize that functions that are accomplished on one server may be partitioned and accomplished on multiple servers that are operatively connected by a computer network by means of appropriate inter process communication. In addition, the access of the website can be by means of an Internet browser accessing a secure or public page or by means of a client program running on a local computer that is connected over a computer network to the server. A data message and data upload or download can be delivered over the Internet using typical protocols, including TCP/IP, HTTP, SMTP, RPC, FTP or other kinds of data communication protocols that permit processes running on two remote computers to exchange information by means of digital network communication. As a result a data message can be a data packet transmitted from or received by a computer containing a destination network address, a destination process or application identifier, and data values that can be parsed at the destination computer located at the destination network address by the destination application in order that the relevant data values are extracted and used by the destination application.

It should be noted that the flow diagrams are used herein to demonstrate various aspects of the invention, and should not be construed to limit the present invention to any particular logic flow or logic implementation. The described logic may be partitioned into different logic blocks (e.g., programs, modules, functions, or subroutines) without changing the overall results or otherwise departing from the true scope of the invention. Oftentimes, logic elements may be added, modified, omitted, performed in a different order, or implemented using different logic constructs (e.g., logic gates, looping primitives, conditional logic, and other logic con-

12

structs) without changing the overall results or otherwise departing from the true scope of the invention.

The method described herein can be executed on a computer system, generally comprised of a central processing unit (CPU) that is operatively connected to a memory device, data input and output circuitry (IO) and computer data network communication circuitry. Computer code executed by the CPU can take data received by the data communication circuitry and store it in the memory device. In addition, the CPU can take data from the I/O circuitry and store it in the memory device. Further, the CPU can take data from a memory device and output it through the IO circuitry or the data communication circuitry. The data stored in memory may be further recalled from the memory device, further processed or modified by the CPU in the manner described herein and restored in the same memory device or a different memory device operatively connected to the CPU including by means of the data network circuitry. The memory device can be any kind of data storage circuit or magnetic storage or optical device, including a hard disk, optical disk or solid state memory.

Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held, laptop or mobile computer or communications devices such as cell phones and PDA's, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

Computer program logic implementing all or part of the functionality previously described herein may be embodied in various forms, including, but in no way limited to, a source code form, a computer executable form, and various intermediate forms (e.g., forms generated by an assembler, compiler, linker, or locator.) Source code may include a series of computer program instructions implemented in any of various programming languages (e.g., an object code, an assembly language, or a high-level language such as FORTRAN, C, C++, JAVA, or HTML) for use with various operating systems or operating environments. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (e.g., via an interpreter), or the source code may be converted (e.g., via a translator, assembler, or compiler) into a computer executable form.

The invention may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. The computer program and data may be fixed in any form (e.g., source code form, computer executable form, or an intermediate form) either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed hard disk), an optical memory device (e.g., a CD-ROM or DVD), a PC card (e.g., PCMCIA card), or other memory device. The computer program and data may be fixed in any form in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies, networking technologies, and inter-networking technologies. The computer program and data may be distributed in any form as a removable storage

US 8,494,967 B2

13

medium with accompanying printed or electronic documentation (e.g., shrink wrapped software or a magnetic tape), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web.) It is appreciated that any of the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices. Practitioners of ordinary skill will recognize that the invention may be executed on one or more computer processors that are linked using a data network, including, for example, the Internet. In another embodiment, different steps of the process can be executed by one or more computers and storage devices geographically separated by connected by a data network in a manner so that they operate together to execute the process steps. In one embodiment, a user's computer can run an application that causes the user's computer to transmit a stream of one or more data packets across a data network to a second computer, referred to here as a server. The server, in turn, may be connected to one or more mass data storage devices where the database is stored. The server can execute a program that receives the transmitted packet and interpret the transmitted data packets in order to extract database query information. The server can then execute the remaining steps of the invention by means of accessing the mass storage devices to derive the desired result of the query. Alternatively, the server can transmit the query information to another computer that is connected to the mass storage devices, and that computer can execute the invention to derive the desired result. The result can then be transmitted back to the user's computer by means of another stream of one or more data packets appropriately addressed to the user's computer.

The described embodiments of the invention are intended to be exemplary and numerous variations and modifications will be apparent to those skilled in the art. All such variations and modifications are intended to be within the scope of the present invention as defined in the appended claims. Although the present invention has been described and illustrated in detail, it is to be clearly understood that the same is by way of illustration and example only, and is not to be taken by way of limitation. It is appreciated that various features of the invention which are, for clarity, described in the context of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable combination. It is appreciated that the particular embodiment described in the specification is intended only to provide an extremely detailed disclosure of the present invention and is not intended to be limiting.

Modifications of the above disclosed apparatus and methods which fall within the scope of the invention will be readily apparent to those of ordinary skill in the art. Accordingly, while the present invention has been disclosed in connection with exemplary embodiments thereof, it should be understood that other embodiments may fall within the spirit and scope of the invention, as defined by the following claims.

14

What is claimed:

1. A method by a server system for obtaining visual validation of the possession of a purchased electronic ticket on a user's computer device for presentation to a ticket taker comprising:

receiving from the user's computer device a request to verify purchase of a previously purchased electronic ticket and to obtain a visual validation display object that confirms that the user possesses the previously purchased electronic ticket for utilization of a service monitored by the ticket taker, the visual validation display object configured to be readily recognizable visually by the ticket taker;

receiving from the user's computer device a token associated with the received request;

determining whether a token associated with the purchased electronic ticket has been stored in a data record associated with the received request, and if it has, whether the received token is valid; and

in dependence on the determination that the received token is valid, causing an activation of the purchased electronic ticket by transmitting to the user's computer device a data file comprising the visual validation display object that causes upon visual recognition by the ticket taker, the user to be permitted to utilize the service monitored by the ticket taker.

2. The method of claim 1 further comprising:

in response to the determining whether a token associated with the purchased electronic ticket has been stored results in a determination that no such token has been stored, initiating confirmation that the purchased electronic ticket has been purchased;

in dependence on such confirmation, storing a token in the data record associated with the purchased electronic ticket; and

transmitting to the user's computer device a visual validation display object corresponding to the purchased electronic ticket.

3. The method of claim 1 further comprising:

storing in the data record associated with the purchased electronic ticket a data value representing a predetermined lock time;

determining whether a duration of time from the transmission of the visual validation display object to the predetermined lock time has expired; and

in dependence on such determination, permitting or not permitting the visual validation display object to be transmitted to the user's computer device.

4. The method of claim 1 further comprising:

transmitting an authorization key to the user's computer device that transmitted the received request.

5. The method of claim 4 further comprising:

encrypting the visual validation display object using the authorization key.

6. The method of claim 4 further comprising:

encrypting the visual validation display object with a public key of a public/private key pair for which the transmitted authorization key is an associated private key.

7. The method of claim 1 further comprising:

establishing a persistent channel between the server system and the user's computer device, the persistent channel being configured to permit the server system to push data to the user's computer device in the absence of a specific request for such data being initiated by the user's computer device.

US 8,494,967 B2

15

8. The method of claim 7 further comprising:
transmitting a command to the user's computer device that
causes the transmitted visual validation display object to
be automatically deleted from the user's computer
device. 5

9. The method of claim 7 further comprising:
transmitting commands that cause the server system to
control a computer process operating on the user's com-
puter device in order to cause the user's computer device 10
to
receive the visual validation display object,
display the validation display visual object on the user's
computer device, and
automatically delete the validation display visual object. 15

10. The method of claim 7 where the persistent channel is
a bi-directional and full-duplex communications channel.

11. The method of claim 7 where the step of transmitting
the visual validation display object is further comprised of:
transmitting in a manner to cause the visual validation 20
display object to be automatically displayed on a screen
without the user having to input a command to cause the
transmission of the validating visual object.

12. The method of claim 7 further comprising:
transmitting to the user's computer device through the 25
persistent channel a visual image comprising one of an
advertisement or a discount coupon.

13. The method of claim 12 further comprising:
selecting a visual image for transmission to the user's
computer device from a plurality of stored visual 30
images, said selection step made in dependence on data
associated with the purchased electronic ticket.

14. The method of claim 13 where the selection step is
further comprised of determining predetermined features of
the validated ticket or purchasing transaction and then mak- 35
ing a selection on the basis of those features.

15. The method of claim 7 further comprising:
transmitting an image that encodes a data value that cor-
responds to data representing an indicia of identity of the
persistent channel. 40

16. The method of claim 15 further comprising:
receiving from the user's computer device a request to
provide a payment authorization, and in response, per-
forming the transmitting an image step;
receiving a request to verify a purchase transaction, said 45
request containing a challenge data;
determining whether the challenge data corresponds to the
identity of the persistent channel used to transmit the
image; and
causing a payment to be made to a payment entity associ- 50
ated with the received request to verify the purchase
transaction.

17. A non-transitory computer readable data storage
medium containing computer program code that when loaded
and executed by a computer system causes the computer 55
system to perform a method for obtaining visual validation
of the possession of a purchased electronic ticket on a user's
computer device for presentation to a ticket taker comprising
the steps of:
receiving from the user's computer device a request to 60
verify purchase of a previously purchased electronic
ticket and to obtain a visual validation display object that
confirms that the user possesses the previously pur-
chased and valid electronic ticket for utilization of a
service monitored by the ticket taker, the visual valida- 65
tion display object configured to be readily recognizable
visually by the ticket taker;

16

receiving from the user's computer device a token associ-
ated with the received request;
determining whether a token associated with the purchased
electronic ticket has been stored in a data record associ-
ated with the received request, and if it has, whether the
received token is valid; and
in dependence on the determination that the received token
is valid, causing an activation of the purchased elec-
tronic ticket by transmitting to the user's computer
device a data file comprising the visual validation dis-
play object that causes upon visual recognition by the
ticket taker, the user to be permitted to utilize the service
monitored by the ticket taker.

18. A system for obtaining visual validation of the posses-
sion of a purchased electronic ticket on a user's computer
device for presentation to a ticket taker comprising one or
more computers operatively connected that are configured to:
receive from the user's computer device a request to verify
purchase of a previously purchased electronic ticket and
to obtain a visual validation display object that confirms
that the user possesses the previously purchased and
valid electronic ticket for utilization of a service moni-
tored by the ticket taker, the visual validation display
object configured to be readily recognizable visually by
the ticket taker;
receive from the user's computer device a token associated
with the received request;
determine whether a token associated with the purchased
electronic ticket has been stored in a data record associ-
ated with the received request, and if it has, whether the
received token is valid; and
in dependence on the determination that the received token
is valid, cause an activation of the purchased electronic
ticket by transmitting to the user's computer device a
data file comprising the visual validation display object
that causes upon visual recognition by the ticket taker,
the user to be permitted to utilize the service monitored
by the ticket taker.

19. The system of claim 18 where the one or more com-
puters are further configured to:
responsive to the determination that no token associated
with the purchased electronic ticket has been stored,
initiate confirmation that the purchased electronic ticket
has been purchased;
in dependence on such confirmation, store a token in the
data record associated with the purchased electronic
ticket; and
transmit to the user's computer device a visual validation
display object corresponding to the purchased electronic
ticket.

20. The system of claim 18 where the one or more com-
puters are further configured to:
store in the data record associated with the purchased elec-
tronic ticket a data value representing a predetermined
lock time; and
determine whether a duration of time from the transmis-
sion of the visual validation display object to the prede-
termined lock time has expired; and
in dependence on such determination, permit or not permit
the visual validation display object to be transmitted to
the user's computer device.

21. The system of claim 18 where the one or more com-
puters are further configured to:
transmit an authorization key to the user's computer device
that transmitted the received request.

US 8,494,967 B2

17

22. The system of claim 21 where the one or more computers are further configured to:

encrypt the visual validation display object using the authorization key.

23. The system of claim 21 where the one or more computers are further configured to:

encrypt the visual validation display object with a public key of a public/private key pair for which the transmitted authorization key is an associated private key.

24. The system of claim 18 where the one or more computers are further configured to:

establish a persistent channel between a server system and the user's computer device, the persistent channel being configured to permit the server system to push data to the user's computer device in the absence of a specific request for such data being initiated by the user's computer device.

25. The system of claim 24 where the one or more computers are further configured to:

transmit a command to the user's computer device that causes the transmitted visual validation display object to be automatically deleted from the user's computer device.

26. The system of claim 24 where the one or more computers are further configured to:

transmit commands that cause the server system to control a computer process operating on the user's computer device in order to cause the user's computer device to receive the visual validation display object, display the validation display visual object on the user's computer device, and automatically delete the validation display visual object.

27. The system of claim 24 where the persistent channel is a bi-directional and full-duplex communications channel.

28. The system of claim 24 where the one or more computers are further configured to:

transmit in a manner to cause the visual validation display object to be automatically displayed on a screen without the user having to input a command to cause the transmission of the validating visual object.

18

29. The system of claim 24 where the one or more computers are further configured to:

transmit to the device through the persistent channel a visual image comprising one of an advertisement or a discount coupon.

30. The system of claim 29 where the one or more computers are further configured to:

select a visual image for transmission to the device from a plurality of stored visual images, said selection step made in dependence on data associated with the purchased electronic ticket.

31. The system of claim 30 where the one or more computers are further configured to select a visual image by means of determining predetermined features of the validated ticket or purchasing transaction and then making a selection on the basis of those features.

32. The system of claim 24 where the one or more computers are further configured to:

transmit an image that encodes a data value that corresponds to data representing an indicia of identity of the persistent channel.

33. The system of claim 32 where the one or more computers are further configured to:

receive from the user device a request to provide a payment authorization, and in response, performing the transmitting an image step;

receive a request to verify a purchase transaction, said request containing a challenge data;

determine whether the challenge data corresponds to the identity of the persistent channel used to transmit the image; and

cause a payment to be made to a payment entity associated with the received request to verify the purchase transaction.

34. The system of claim 18 where the visual validation display object is an animation that operates in reaction to a touch of the user's computer device screen.

* * * * *



US00923993B2

(12) **United States Patent**
Bergdale et al.

(10) **Patent No.:** **US 9,239,993 B2**
(45) **Date of Patent:** **Jan. 19, 2016**

(54) **METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH VISUAL DISPLAY**

(58) **Field of Classification Search**
None
See application file for complete search history.

(71) Applicant: **ByteMark, Inc.**, New York, NY (US)

(56) **References Cited**

(72) Inventors: **Micah Bergdale**, New York, NY (US);
Matthew Grasser, New York, NY (US);
Nicholas Ihm, Brooklyn, NY (US);
Samuel Krueckeberg, New York, NY (US);
Gregory Valyer, Highland Park, IL (US)

U.S. PATENT DOCUMENTS

4,193,114 A * 3/1980 Benini 705/13
5,253,166 A 10/1993 Dettelbach
5,465,084 A * 11/1995 Cottrell 340/5.27
5,559,961 A * 9/1996 Blonder 726/18

(Continued)

(73) Assignee: **BYTEMARK, INC.**

FOREIGN PATENT DOCUMENTS

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

GB 2390211 12/2003
GB 2417358 2/2006

(Continued)

(21) Appl. No.: **13/901,243**

OTHER PUBLICATIONS

(22) Filed: **May 23, 2013**

Scott Boyter, "Aeritas tried to fill void until 3G wireless is ready; Mobile boarding pass is just one application being tested", all pages, Dallah Forth Worth TechBiz, Feb. 19, 2011.*

(Continued)

(65) **Prior Publication Data**

US 2013/0262163 A1 Oct. 3, 2013

Related U.S. Application Data

(63) Continuation-in-part of application No. 13/046,413, filed on Mar. 11, 2011, and a continuation of application No. 13/475,881, filed on May 18, 2012, now Pat. No. 8,494,967, which is a continuation-in-part of application No. 13/110,709, filed on May 18, 2011.

(51) **Int. Cl.**
G06Q 40/00 (2012.01)
G06Q 10/02 (2012.01)
G06Q 20/04 (2012.01)
G06Q 20/32 (2012.01)

(52) **U.S. Cl.**
CPC **G06Q 10/02** (2013.01); **G06Q 20/0457** (2013.01); **G06Q 20/3274** (2013.01)

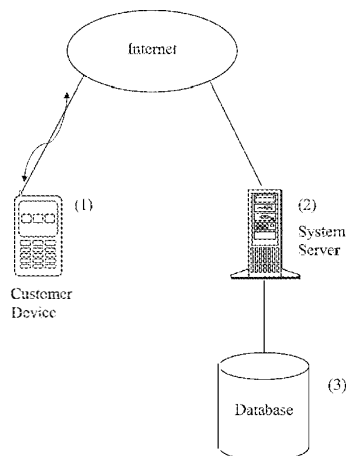
Primary Examiner — Calvin Cheung

(74) *Attorney, Agent, or Firm* — Jennifer Meredith, Esq.;
Meredith & Keyhani, PLLC

(57) **ABSTRACT**

This invention discloses a novel system and method for distributing electronic ticketing such that the ticket is verified at the entrance to venues by means of an animation or other human perceptible verifying visual object that is selected by the venue for the specific event. This removes the need to use a bar-code scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders. The system also can permit ticket purchase verification in the absence of a network connection during verification.

26 Claims, 16 Drawing Sheets



US 9,239,993 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

5,590,038 A *	12/1996	Pitroda	705/41	2003/0069827 A1 *	4/2003	Gathman et al.	705/37
5,621,797 A	4/1997	Rosen		2003/0105641 A1 *	6/2003	Lewis	705/1
5,777,305 A	7/1998	Smith		2003/0105954 A1	6/2003	Immonen	
5,789,732 A *	8/1998	McMahon et al.	235/487	2003/0105969 A1	6/2003	Matsui	
5,907,830 A	5/1999	Engel		2003/0154169 A1	8/2003	Yanai	
5,918,909 A	7/1999	Fiala		2003/0163787 A1	8/2003	Hay	
6,023,679 A	2/2000	Acebo		2003/0172037 A1 *	9/2003	Jung et al.	705/64
6,023,688 A *	2/2000	Ramachandran et al.	705/44	2003/0200184 A1	10/2003	Dominguez	
6,085,976 A *	7/2000	Sehr	235/384	2003/0229790 A1	12/2003	Russell	
6,175,922 B1 *	1/2001	Wang	713/182	2003/0233276 A1	12/2003	Pearlman	
6,251,017 B1	6/2001	Leason		2004/0019564 A1	1/2004	Goldthwaite	
6,315,195 B1 *	11/2001	Ramachandran	235/380	2004/0019792 A1 *	1/2004	Funamoto et al.	713/179
6,373,587 B1 *	4/2002	Sansone	358/1.15	2004/0030081 A1	2/2004	Hegi	
6,393,305 B1 *	5/2002	Ulvinen et al.	455/563	2004/0030091 A1	2/2004	McCullough	
6,454,174 B1	9/2002	Sansone		2004/0030658 A1	2/2004	Cruz	
6,473,739 B1 *	10/2002	Showghi et al.	705/15	2004/0085351 A1 *	5/2004	Tokkonen	345/741
6,484,182 B1	11/2002	Dunphy		2004/0101158 A1	5/2004	Butler	
6,493,110 B1 *	12/2002	Roberts	358/1.2	2004/0111373 A1	6/2004	Iga	
6,496,809 B1 *	12/2002	Nakfoor	705/80	2004/0148253 A1	7/2004	Shin	
6,685,093 B2 *	2/2004	Challa et al.	235/462.46	2004/0169589 A1	9/2004	Lea	
6,775,539 B2	8/2004	Deshpande		2004/0186884 A1	9/2004	Dutordoir	
6,961,858 B2	11/2005	Fransdonk		2004/0210476 A1	10/2004	Blair	
6,997,384 B2	2/2006	Hara		2004/0224703 A1	11/2004	Takaki	
7,017,806 B2	3/2006	Peterson		2004/0250138 A1 *	12/2004	Schneider	713/202
7,020,635 B2	3/2006	Hamilton		2005/0059339 A1	3/2005	Honda	
7,024,807 B2	4/2006	Street		2005/0060554 A1 *	3/2005	Donoghue	713/183
7,044,362 B2 *	5/2006	Yu	235/375	2005/0070257 A1	3/2005	Saarenen	
7,080,049 B2	7/2006	Truitt		2005/0109838 A1	5/2005	Linlor	
7,090,128 B2	8/2006	Farley		2005/0111723 A1	5/2005	Hannigan	
7,093,130 B1	8/2006	Kobayashi		2005/0212760 A1 *	9/2005	Marvit et al.	345/156
7,103,572 B1 *	9/2006	Kawaguchi et al.	705/40	2005/0240589 A1 *	10/2005	Altenhofen	G06F 21/10 709/229
7,107,462 B2	9/2006	Fransdonk		2005/0253817 A1 *	11/2005	Rytivaara et al.	345/173
7,134,087 B2	11/2006	Bushold		2005/0272473 A1	12/2005	Sheena	
7,150,045 B2	12/2006	Koelle		2006/0161446 A1 *	7/2006	Fyfe et al.	705/1
7,158,939 B2	1/2007	Goldstein		2006/0174339 A1 *	8/2006	Tao	726/18
7,174,462 B2 *	2/2007	Pering et al.	713/182	2006/0206724 A1	9/2006	Schaufele	
7,191,221 B2	3/2007	Schatz		2006/0293929 A1	12/2006	Wu	
7,263,506 B2	8/2007	Lee et al.		2007/0012765 A1 *	1/2007	Trinquet et al.	235/382
7,315,944 B2	1/2008	Dutta		2007/0017979 A1	1/2007	Wu	
7,386,517 B1	6/2008	Donner		2007/0022058 A1	1/2007	Labrou	
7,392,226 B1	6/2008	Sasaki		2007/0032225 A1 *	2/2007	Konicek et al.	455/417
7,395,506 B2 *	7/2008	Tan et al.	715/741	2007/0136213 A1 *	6/2007	Sansone et al.	705/401
7,493,261 B2	2/2009	Chen		2007/0150842 A1 *	6/2007	Chaudhri et al.	715/863
7,520,427 B2	4/2009	Boyd		2007/0156443 A1 *	7/2007	Gurvey	705/1
7,529,934 B2	5/2009	Fujisawa		2007/0192590 A1	8/2007	Pomerantz	
7,567,910 B2	7/2009	Hasegawa et al.		2007/0260543 A1 *	11/2007	Chappuis	705/44
7,587,502 B2	9/2009	Crawford		2007/0271455 A1	11/2007	Nakano	
7,617,975 B2 *	11/2009	Wada et al.	235/382	2008/0071587 A1	3/2008	Granucci	
7,711,586 B2	5/2010	Aggarwal		2008/0071637 A1	3/2008	Saarenen et al.	
7,933,589 B1 *	4/2011	Mamdani et al.	455/414.1	2008/0120127 A1 *	5/2008	Stoffelsma et al.	705/1
7,967,211 B2	6/2011	Challa		2008/0201576 A1 *	8/2008	Kitagawa et al.	713/168
8,010,128 B2	8/2011	Silverbrook		2008/0201769 A1	8/2008	Finn	
8,016,187 B2	9/2011	Frantz		2008/0227518 A1 *	9/2008	Wiltshire	G07F 17/3227 463/17
8,019,365 B2	9/2011	Fisher		2008/0263077 A1 *	10/2008	Boston	707/102
8,473,342 B1	6/2013	Roberts		2008/0288302 A1 *	11/2008	Daouk et al.	705/5
8,583,511 B2	11/2013	Hendrickson		2008/0308638 A1	12/2008	Hussey	
2001/0005840 A1 *	6/2001	Verkama	705/67	2009/0284482 A1 *	11/2009	Chin	345/173
2001/0014870 A1	8/2001	Saito		2010/0017872 A1 *	1/2010	Goertz et al.	726/16
2001/0016825 A1 *	8/2001	Pugliese et al.	705/5	2010/0121766 A1	5/2010	Sugaya	
2001/0044324 A1 *	11/2001	Carayiannis et al.	455/564	2010/0211452 A1	8/2010	D'Angelo	
2001/0051787 A1	12/2001	Haller		2010/0268649 A1 *	10/2010	Roos et al.	705/50
2001/0052545 A1 *	12/2001	Serebrennikov	235/462.46	2010/0279610 A1	11/2010	Bjorhn	
2001/0054111 A1 *	12/2001	Lee et al.	709/245	2010/0306718 A1 *	12/2010	Shim et al.	715/863
2002/0016929 A1	2/2002	Harashima		2010/0322485 A1 *	12/2010	Riddiford	382/115
2002/0023027 A1 *	2/2002	Simonds	705/26	2011/0040585 A1	2/2011	Roxburgh et al.	
2002/0040308 A1	4/2002	Hasegawa		2011/0068165 A1 *	3/2011	Dabosville	235/375
2002/0040346 A1	4/2002	Kwan		2011/0078440 A1 *	3/2011	Feng	G06Q 10/02 713/168
2002/0060246 A1 *	5/2002	Gobburu et al.	235/462.46	2011/0136472 A1 *	6/2011	Rector et al.	455/411
2002/0065713 A1	5/2002	Awada		2011/0153495 A1	6/2011	Dixon	
2002/0065783 A1	5/2002	Na		2011/0251910 A1	10/2011	Dimmick	
2002/0094090 A1 *	7/2002	Iino	380/282	2011/0283241 A1 *	11/2011	Miller et al.	715/863
2002/0138346 A1	9/2002	Kodaka		2011/0307381 A1	12/2011	Kim	
2002/0196274 A1 *	12/2002	Comfort et al.	345/741	2012/0006891 A1	1/2012	Zhou	
2003/0036929 A1	2/2003	Vaughan		2012/0030047 A1	2/2012	Fuentes	
2003/0066883 A1 *	4/2003	Yu	235/382	2012/0133484 A1 *	5/2012	Griffin	340/5.54

US 9,239,993 B2

Page 3

(56)

References Cited

U.S. PATENT DOCUMENTS

2012/0136698 A1 5/2012 Kent
 2012/0166298 A1 6/2012 Smith
 2013/0279757 A1* 10/2013 Kephart 382/105

FOREIGN PATENT DOCUMENTS

JP H11145952 A 5/1999
 JP 2003-187272 A * 7/2003 G07B 1/00
 TW 200825968 A * 6/2008 G06Q 30/00
 WO 2007139348 A1 12/2007
 WO 2008113355 9/2008
 WO 2009141614 11/2009
 WO 2011044899 4/2011

OTHER PUBLICATIONS

Joanna Elachi, "Lufthansa Debuts Barcode Check-in and Boarding", all pages, CommWeb.com, May 25, 2001.*

"Aeritas launches secure wireless check-in with barcode", all pages, m-Travel.com, Nov. 9, 2001.*

"Aeritas Launches Wireless Check-in and Security Service", all pages, MBusiness Daily, Nov. 8, 2001.*

"New Fast Track Wireless Check-In and Security Solution", all pages, aerias.com, retrieved Feb. 5, 2002.*

Machine English Translation of JP2003-187272A.*

Starnberger et al., "QR-TAN: Secure Mobile Transaction Authentication," area, pp. 578-583, 2009 International Conference on Availability, Reliability and Security, 2009.

"New Fast Track Wireless Check-In and Security Solution", all pages, aerias.com, retrieved Feb. 5, 2002.

Chun-Te Chen; Te-Chung Lu, "A mobile ticket validation by VSS teach with time stamp" Mar. 28-31, 2004.

Hussin, W.H.; Coulton, P; Edwards, R., "Mobile ticketing system employing TrustZone technology" Jul. 11-13, 2005.

Jong-Sik Moon; Sun-Ho Lee; Im-Yeong Lee; Sang-Gu Byeon, "Authentication Protocol Using Authorization Ticket in Mobile Network Service Environment" Aug. 11-13, 2010.

Stephanie Bell, "UK Rail Network to Launch Mobile Train-Ticketing Application" Cardline, Feb. 4, 2011.

Ko Fujimura, Yoshiaki Nakajima, Jun Sekine: "XML Ticket: Generalized Digital Ticket Definition Language" Proceedings of the 3rd Usenix Workshop on Electronic Commerce, Sep. 3, 1998.

* cited by examiner

U.S. Patent

Jan. 19, 2016

Sheet 1 of 16

US 9,239,993 B2

Figure 1.

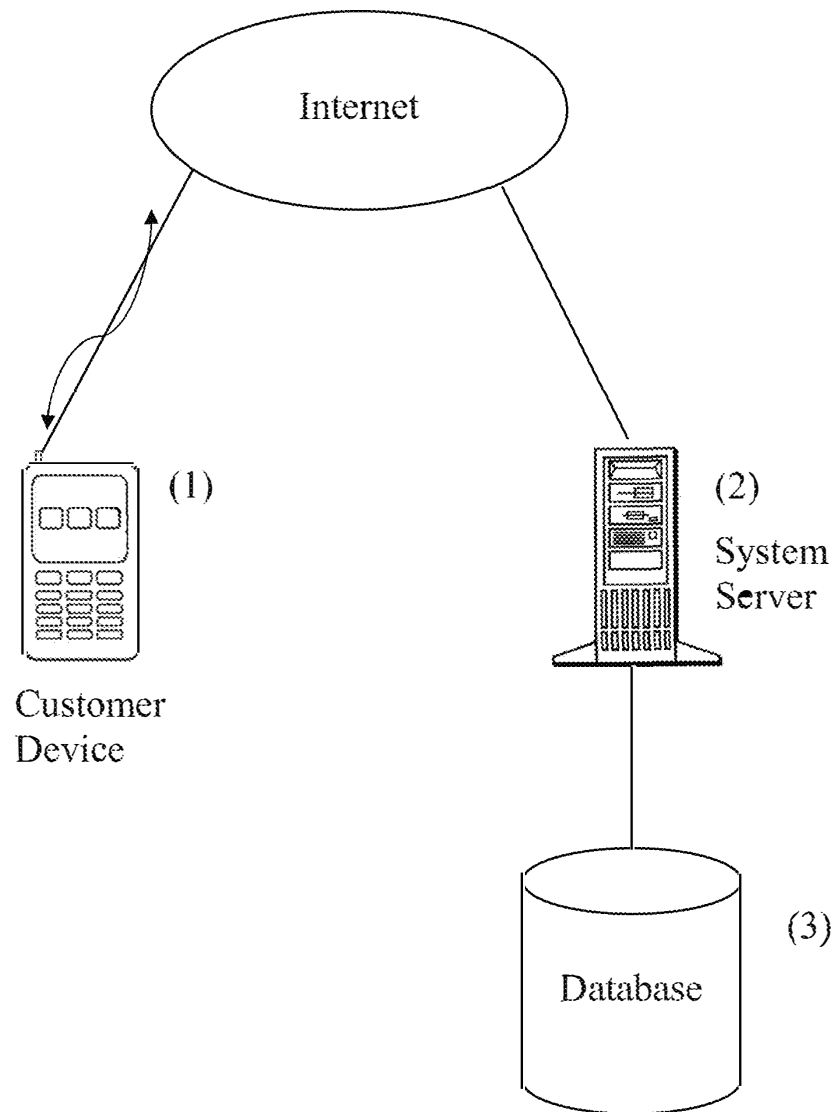


Figure 2

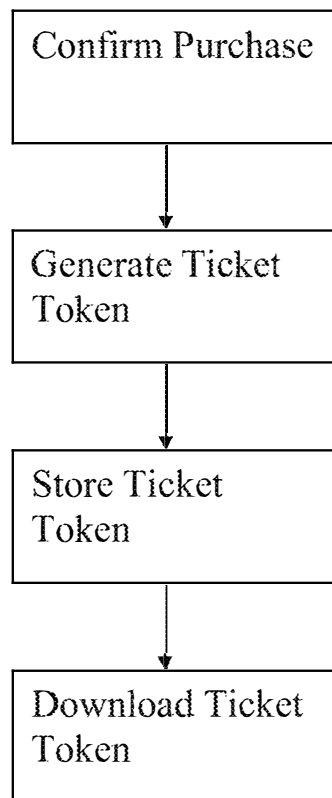
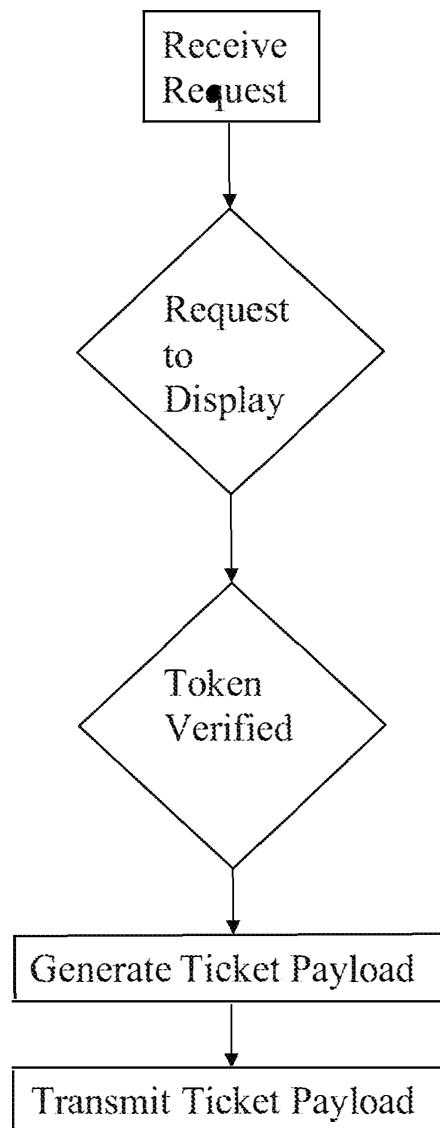


Figure 3



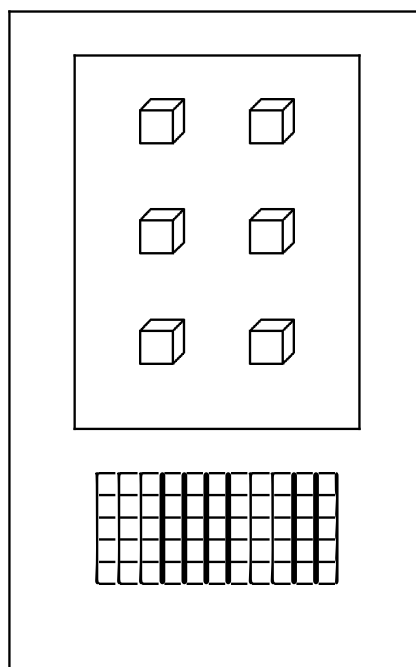
U.S. Patent

Jan. 19, 2016

Sheet 4 of 16

US 9,239,993 B2

Figure 4



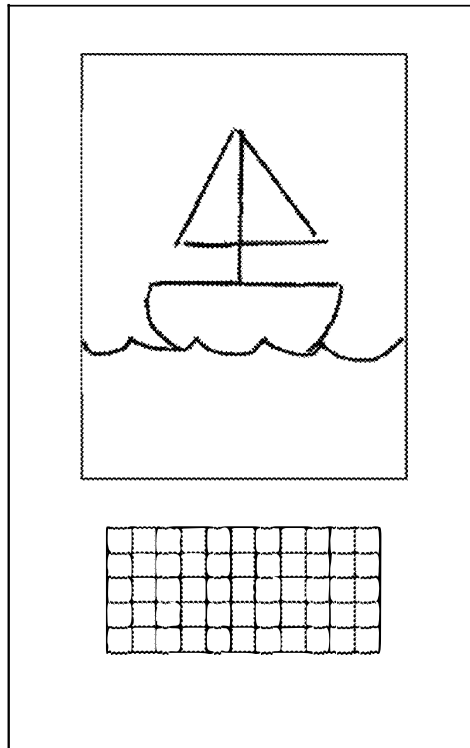
U.S. Patent

Jan. 19, 2016

Sheet 5 of 16

US 9,239,993 B2

Figure 5



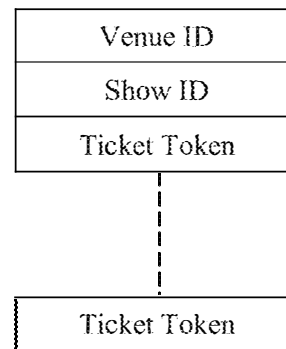
U.S. Patent

Jan. 19, 2016

Sheet 6 of 16

US 9,239,993 B2

Figure 6



U.S. Patent

Jan. 19, 2016

Sheet 7 of 16

US 9,239,993 B2

Figure 7

Venue ID
Username
Password

U.S. Patent

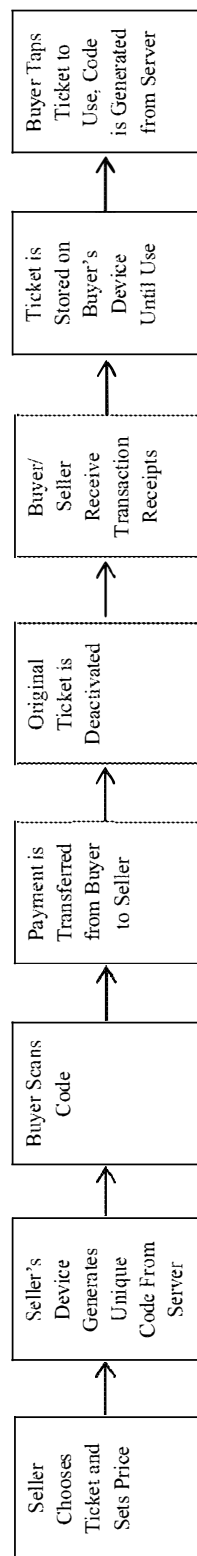
Jan. 19, 2016

Sheet 8 of 16

US 9,239,993 B2

Figure 8

P2P Buying & Selling



U.S. Patent

Jan. 19, 2016

Sheet 9 of 16

US 9,239,993 B2

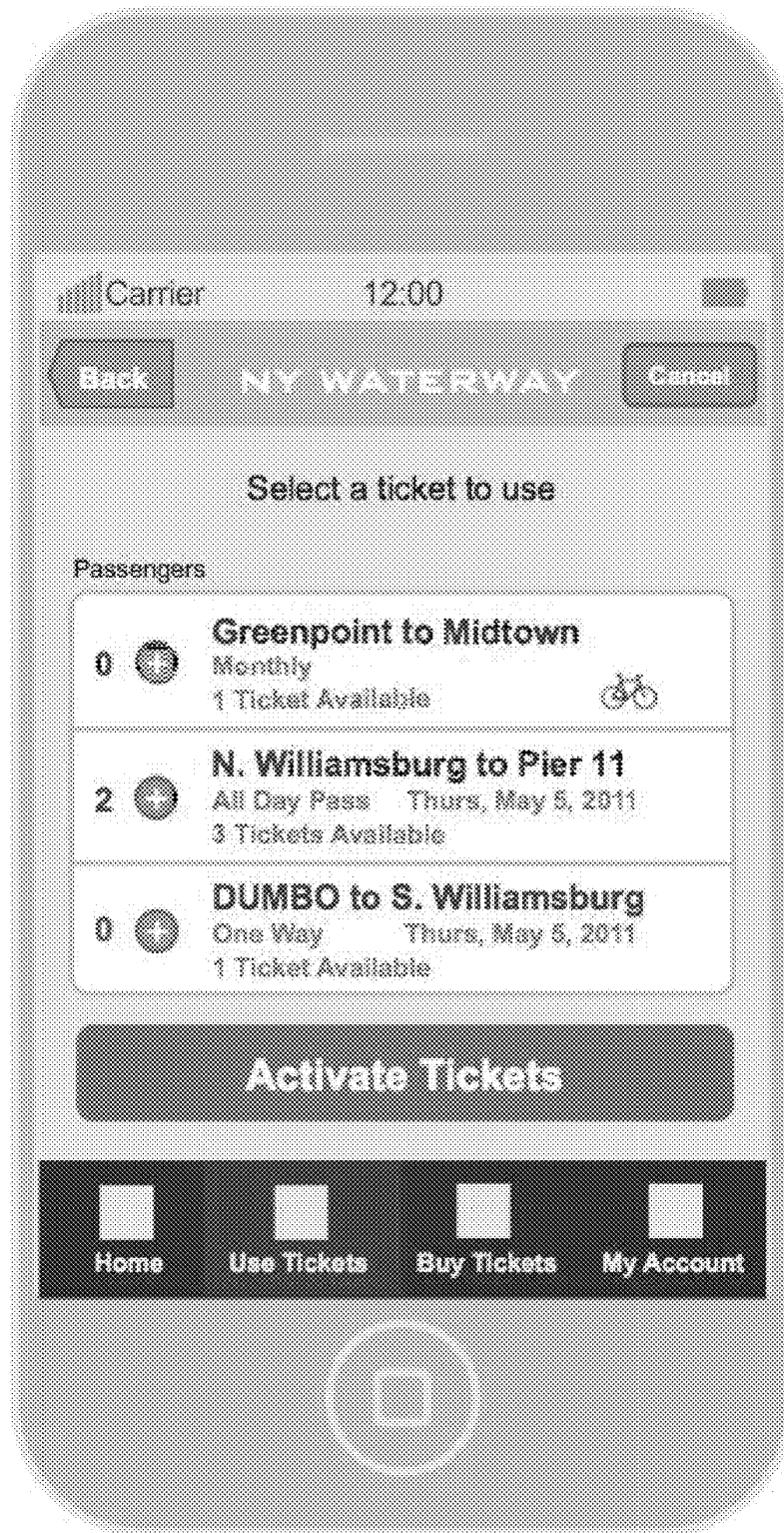


FIGURE 9

U.S. Patent

Jan. 19, 2016

Sheet 10 of 16

US 9,239,993 B2

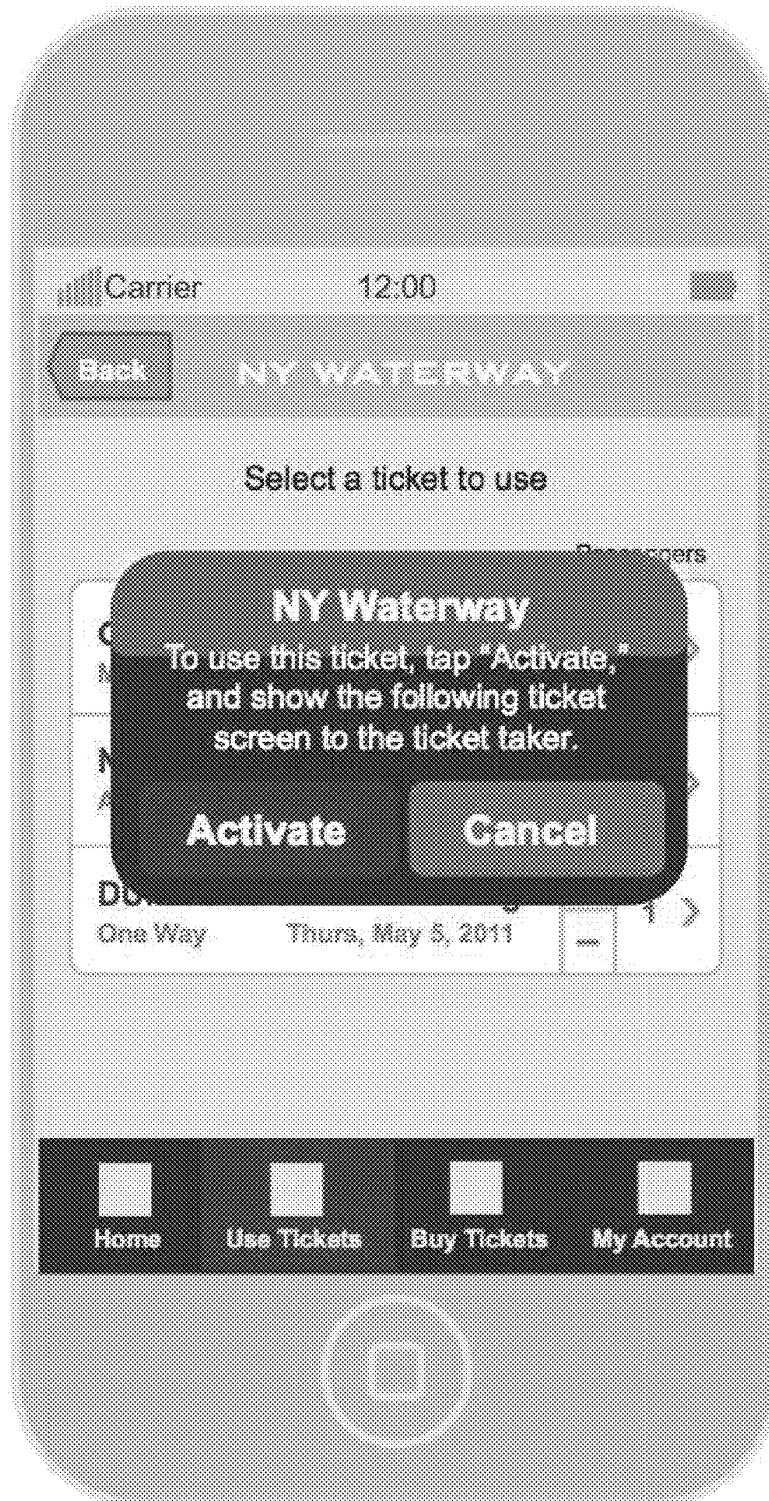


FIGURE 10

U.S. Patent

Jan. 19, 2016

Sheet 11 of 16

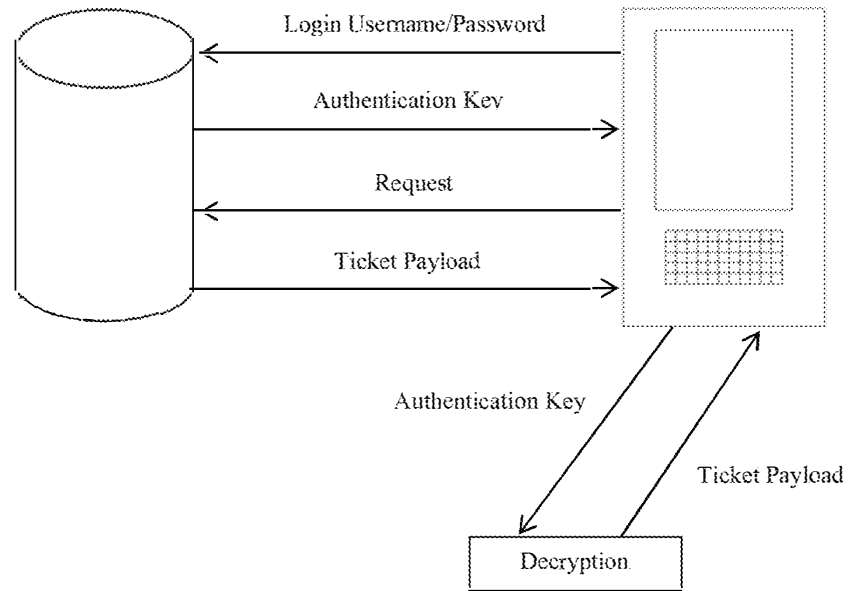
US 9,239,993 B2



FIGURE 11

Appx3328

Figure 12.



U.S. Patent

Jan. 19, 2016

Sheet 13 of 16

US 9,239,993 B2

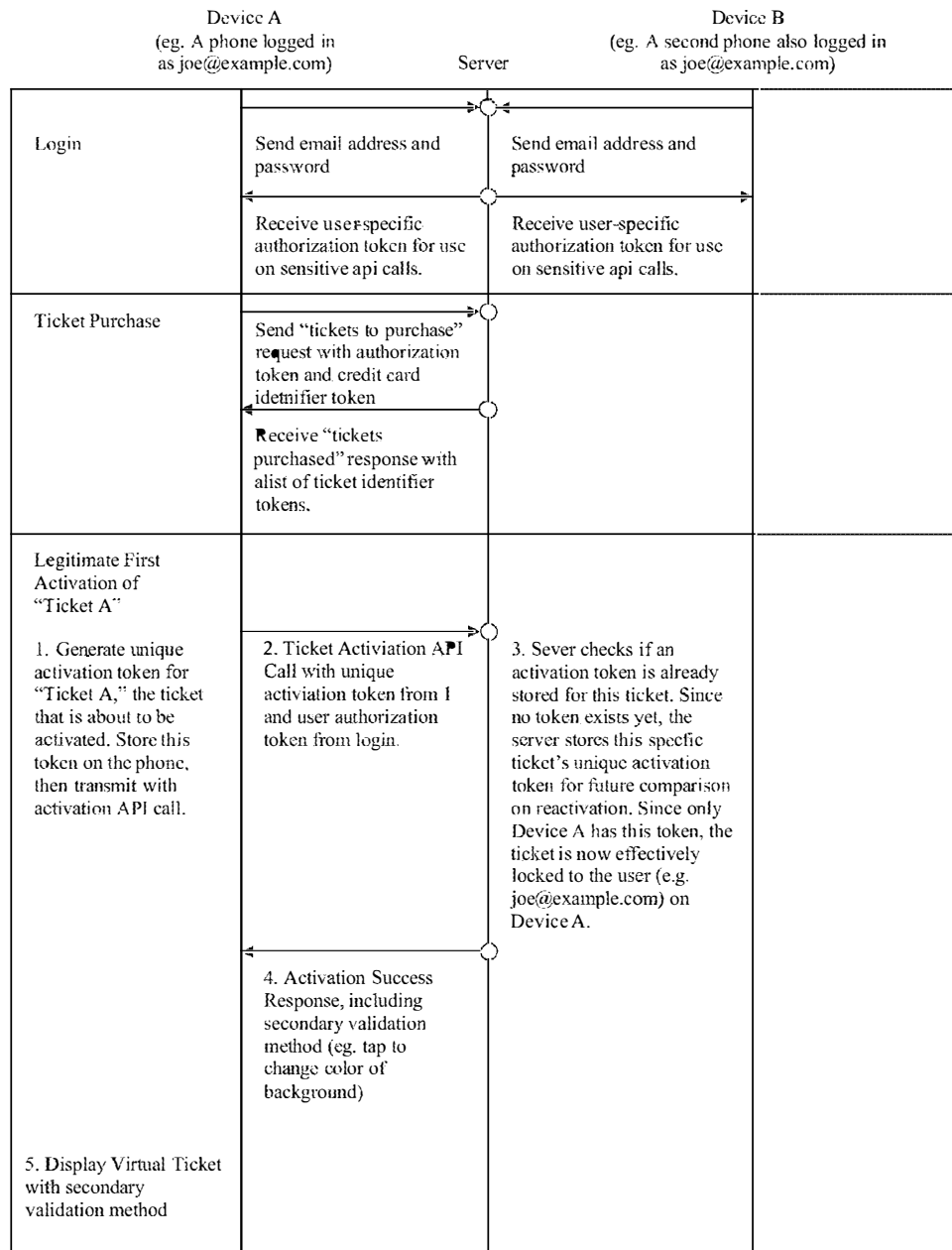


Fig. 13a

U.S. Patent

Jan. 19, 2016

Sheet 14 of 16

US 9,239,993 B2

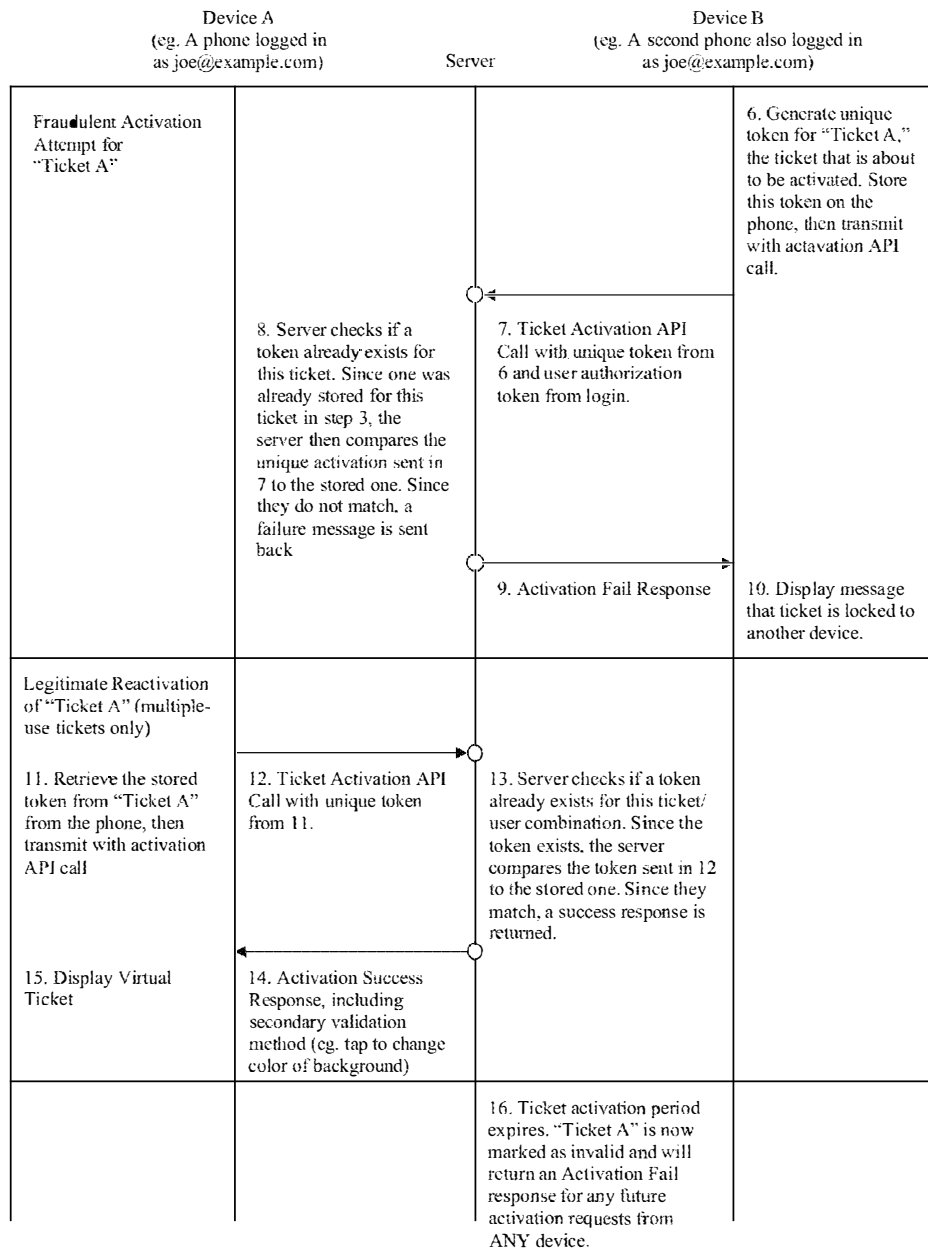


Fig. 13b

U.S. Patent

Jan. 19, 2016

Sheet 15 of 16

US 9,239,993 B2

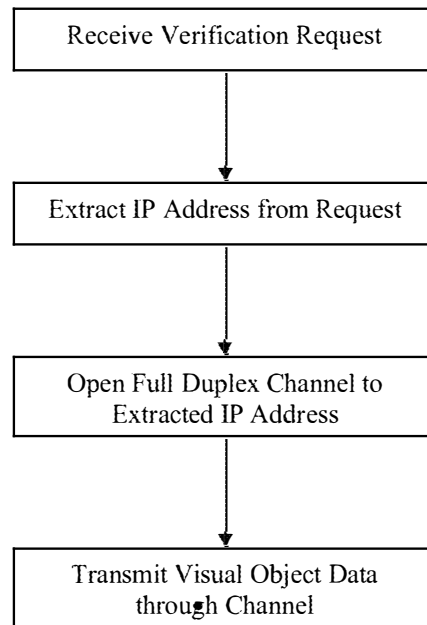


Fig. 14

Appx3332

U.S. Patent

Jan. 19, 2016

Sheet 16 of 16

US 9,239,993 B2

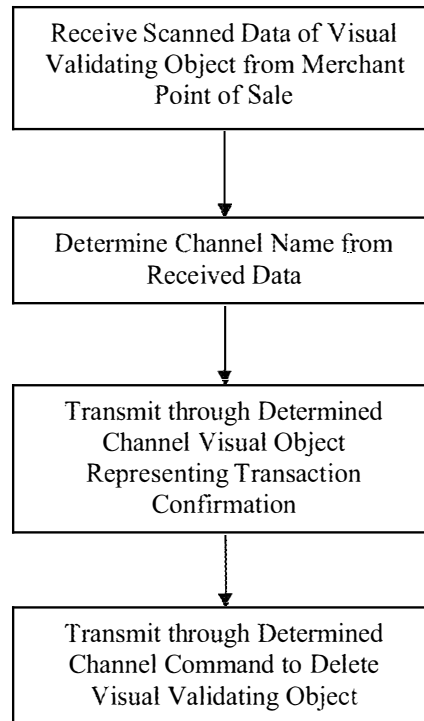


Fig. 15

Appx3333

US 9,239,993 B2

1

METHOD AND SYSTEM FOR DISTRIBUTING ELECTRONIC TICKETS WITH VISUAL DISPLAY

This application claims priority to U.S. patent application Ser. No. 13/475,881 filed on May 18, 2012 as a continuation and herein incorporates that application by reference in its entirety, which further claims priority to U.S. patent application Ser. No. 13/110,709 filed on May 18, 2011 as a Continuation in Part and hereby incorporates that application by reference in its entirety. This application also claims priority to U.S. patent application Ser. No. 13/046,413 filed on Mar. 11, 2011 as a Continuation in Part and hereby incorporates that application by reference in its entirety.

FIELD OF INVENTION

This invention provides a mechanism whereby a venue or other facility that meters usage by means of tickets can distribute tickets electronically and use a visual aid on an electronic device to visually confirm that a person is a valid ticket holder.

BACKGROUND

Venues such as theaters, amusement parks and other facilities that use tickets, for example airlines, ferries and other transportation have a need to use electronic ticketing. Existing systems distribute information that can constitute a ticket, but the verification problem is difficult. In one example of prior art, an electronic ticket is displayed as a bar-code on the recipient's telephone display screen. The telephone is then placed on a scanner that reads the bar-code in order to verify the ticket. The problem with these systems is that the scanning process is fraught with error and the time taken to verify the electronic ticket far exceeds that of the old system: looking at the paper ticket and tearing it in half. Barcode scanners were not designed to read a lit LCD screen displaying a bar code. The reflectivity of the screen can defeat the scanning process. Therefore, there is a need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket. This invention provides for the distribution of an electronic ticket that also contains a visual display that ticket takers can rely on as verification, without using a scanning device.

DESCRIPTION OF THE FIGURES

FIG. 1. Basic architecture.
 FIG. 2. Flow chart for ticket purchase.
 FIG. 3. Flow chart for displaying the verifying visual object.
 FIG. 4. Example validating visual object.
 FIG. 5. Example validating visual object
 FIG. 6. Schematic of event database record.
 FIG. 7. Schematic of authorized user database record.
 FIG. 8. Flow chart for transfer of ticket.
 FIG. 9. Example user interface on user's device.
 FIG. 10. Example user interface showing activation selection screen.
 FIG. 11. Example user interface showing display of validating visual object and other ticketing information.
 FIG. 12. Flowchart for ticket activation process.
 FIG. 13a. Protocol diagram for activation process.
 FIG. 13b. Continued protocol diagram for activation process.

2

FIG. 14. Flowchart for persistent channel.

FIG. 15. Flowchart for persistent channel for purchase verification.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The system operates on one or more computers, typically one or more file servers connected to the Internet and also on a customer's computing device. A customer's device can be a personal computer, mobile phone, mobile handheld device like a Blackberry™ or iPhone™ or any other kind of computing device a user can use to send and receive data messages. The customer's device is used to display the validating visual object.

Conventional electronic tickets display a barcode or QR code on a user's telephone, typically a cellphone or other portable wireless device with a display screen. The problem with this approach is that a barcode scanner has to be used by the ticket taker. Barcode scanners are not highly compatible with LCD screen displays of barcodes. The amount of time that it takes to process an electronic ticket is greater than that of a paper ticket. Sometimes the LCD display does not scan at all and a passenger has to be sent away to get a paper printout of a ticket. Given the potential large crowds that often attend open venues, this is impractical.

In this invention, the ticket is procured electronically and stored on the user's device. However, when the ticket is to be taken the verification is determined by a larger visual object that a human can perceive without a machine scanning it. The particular validating visual object chosen can be constantly changed so that the ticket taker does not have to be concerned that a device displaying the designated validating visual object is invalid. There are many types of visual objects that can be displayed that are easily recognized by a ticket taker. These can include but are not limited to: Patterns of color change, Animations and Geometric patterns. In one embodiment, the validating visual object that is transmitted can be computer code, that when executed by the device, causes the user device to display the desired visual pattern. In another embodiment, the validating visual object is a command that specifies what the visual pattern should be. In that embodiment, the program operating on the user's device receives the command instruction, decodes it, and determines what visual patterns to generate based on the data in the command instruction. In another embodiment, the validating visual object is video or image data transmitted directly from the server to the device for immediate display.

In one embodiment of the invention, the user purchases a ticket from an on-line website. The website sends to the user's device a unique number, referred to as a token. The token is also stored in the ticketing database. When the time comes to present the ticket, the venue can select what visual indicator will be used as the designated validation visual object. The user can then request the validation visual object. The user's device will have an application that launches a user interface. The user can select "validate" or some other equivalent command to cause the application to fetch and download from the ticketing system a data object referred to herein as a ticket payload, which includes a program to run on the user's device. In another embodiment, the ticket payload can be pushed to the device by the venue. As a result, the application transmitted to the user's device is previously unknown to the user and not resident in the user's device. At that point the user's device can execute the program embodied in the ticket payload, which causes the validation visual object to be displayed on the user's device. The ticket taker knows what the

US 9,239,993 B2

3

validating visual object is, and simply looks to see that the user's device is displaying the correct visual object.

Piracy is limited in several ways. First, the ticket holder and their device does not have access to the validating visual object until a time select to be close to the point in time where the ticket has to be presented. Second, the validating visual object is one of an very large number of permutations and therefore cannot be guessed, selected or copied ahead of time. Third, the ticket payload can contain code that destroys the validating visual object in a predetermined period of time after initial display or upon some pre-determined input event. Fourth, a number of security protocols can be utilized to ensure that a copy of the application that executes to display the validating visual object cannot be readily copied or reverse engineered.

Validating Visual Object Displays:

There many kinds of validation displays that can be utilized. The criterion for what constitutes a validating visual object is one that is readily recognizable from human observation, is encapsulated in such a way as to be transmitted to the customer's device with a minimum of network latency or download time, and that can be reasonably secured so as to avoid piracy.

Barcodes and similar codes like the QR code are not validating visual objects because a person looking at them cannot tell one apart from another. Instead, the person has to rely on a barcode scanner and computing device to verify the barcode.

In one embodiment, the period that a particular validating visual object may be used is automatically limited. Examples of validating visual objects include:

1. A color display on the device.
2. A color sequence.
3. An animation that is easily recognized.
4. Animations can include easily recognizable geometric patterns, for example an array of diamonds, or an array of rotating cubes.
5. A human recognizable image.
6. The customer's face as an image.
7. Combinations of the above.

In another embodiment, other images, for example, block letter, can be displayed so that additional information readily apparent to the ticket taker is displayed. For example, a letter can be designated for a Child ticket or a different letter for an Adult ticket.

Referring now to FIG. 1, the customer uses their device (1) to purchase a ticket from the service operating the system server (2) and database (3).

In one embodiment, an authorized user associated with the venue, typically the box office manager, logs into the back-end system through a secure web-page. The authorized user can enter the web-page by entering a username, password and venue identifier. The system maintains a database (3) that associates the venue identifier with a set of usernames and password pairs that are authorized to use the system on behalf of the venue. See FIG. 7. The system checks the database (3) to verify that the venue ID, username and password are consistent with each other. The authorized user can navigate through to a point in the system user interface where a particular show may be selected for ticket taking. The user selects the upcoming show, and then selects from a display of possible validating visual objects. The validating visual object is transmitted to a device viewable by ticket taking staff at the entrances to the venue. The staff then can see the authorized object to accept for the upcoming show.

Ticket holders that have purchased tickets have a data record in the system database that contains the unique token associated with the ticket and other relevant information,

4

including the venueID and an identifier identifying the specific show the ticket is for. See FIG. 6. At the entrance, customers are requested to operate an application on their devices. This application fetches the stored ticket token and transmits that token to the system, preferably over a secure data channel. The database looks up the token to check that the token is valid for the upcoming show. If the token is valid, then the system transmits back to the device a ticket payload. The ticket payload contains computer code that, when operated, displays the selected validating visual object.

The customer can navigate the user interface of the application in order to cause the application to request whether to display the validating visual object. As shown in FIG. 9, one or more available tickets can be displayed on the user interface, which provides the user the ability to select one of the tickets. When the customer properly actuates the user interface, for example, by actuating the "Activate Tickets" button (see FIG. 10), the validating visual object is displayed on the screen of the device. The animation can be presented along with other ticketing information (see FIG. 11). In one embodiment, the device transmits the ticket token to the system with a command indicating that the ticket has been used. In another embodiment, the customer can operate the application and request that the application transmit to the database the condition that the ticket was used. In that embodiment, the user can input a numeric code or password that the application uses to verify that the customer is confirming use of the ticket. In yet another embodiment, after the validating visual object has been launched, a predetermined amount of time later it can be deemed used. At that time, the application can cause the color of the object to be changed so that it indicates that there was a valid ticket, but the ticket was used. This condition is useful in cases where the venue checks tickets during shows while letting customers move around the venue's facilities.

In another embodiment, the purchase of the ticket causes the ticket payload to be downloaded to the customer's device. Likewise, the authorized user for the venue will select a validating visual object for a particular show well in advance of the show. In this case, because a customer may possess the payload some time before its use, precautions must be taken to secure the ticket payload from being hacked so that any similar device can display the validating visual object. While this is a security tradeoff, the benefit is that the customer need not have an Internet connection at a time close to the show-time of the venue.

The use of electronic ticketing provides opportunities that change how tickets can be bought and sold. For example a first customer can purchase a ticket and receive on their device a ticket token. A second customer can purchase that ticket using the system. The first customer can use the application to send a message to the system server indicating that the first customer intends to the web-page indicating that it wants to buy that particular ticket. The system can ask the first customer for a username and password to be associated with the first customer's ticket. If the second customer identifies the first customer's username, the system then can match the two together. At that point, the data record associated with the first customer's ticket is modified so that the ticket token value is changed to a new value. That new ticket token value is then transmitted to the second customer's device. At the same time, the system can operate a typical on-line payment and credit system that secures payment from the second customer and credits the first customer. In one embodiment, the system pays the first customer a discounted amount, retaining the balance as a fee.

US 9,239,993 B2

5

In yet another embodiment, the first customer may be unknown to the second customer. In that embodiment, the first customer simply may indicate to the system, through a message transmitted from the application operating on the device or directly through a web-page, that the first customer is not going to use the ticket and wishes to sell it. At that point, the system can mark the data record associated with the ticket as "available for sale." When the second customer makes a request to purchase a ticket for the same show, the system creates a new ticket token for the second customer and updates the ticket token stored in the data record.

In a general admission type of scenario, the ticketing database is simple: each show has a venue ID, some identifier associated with the show itself, various time indicators, the selected validating visual object, and a list of valid ticket tokens. In a reserved seating arrangement, the ticketing database has a data record associated with a show, as indicated by a show identifier, but each seat has a data record that has a unique show identifier and ticket token, which includes the identity of the seat itself.

In the preferred embodiment, the validating visual object is secured against tampering. One threat model is that a customer who has received a ticket payload would then take the data file comprising the ticket payload and analyze it to detect the actual program code that when executed, produces the validating visual object on the display screen of the device. Once that has been accomplished, the would-be pirate can then re-package the code without any security mechanism and readily distribute it to other device owners, or even cross-compile it to execute on other types of display devices. The preferred embodiment addresses this threat model in a number of ways.

First, the ticket payload can be secured in a region of the device under the control of the telecommunications provider. In this case, the customer cannot access the code comprising the ticket payload. In another embodiment, the ticket payload can be encrypted in such a way that the only decrypting key available is in the secure portion of the telecommunications device. In that embodiment, the key is only delivered when an application running on the secure part of the device confirms that the ticket payload that is executing has not been tampered with, for example, by checking the checksum of its run-time image. At that point, the key can be delivered to the ticket payload process so that the validating visual object is displayed on the device.

Second, the selected animation is packaged for each device. That is, the code that operates to display the validating visual object itself operates certain security protocols. The phone transmits a ticket transaction request. The request includes a numeric value unique to the device, for example, an IMEI number. Other embodiments use the UDID or hardware serial number of the device instead of or in combination with the IMEI number. The system server then generates the ticket token using the IMEI number and transmits that value to that device. In addition, the ticket payload is created such that it expects to read the correct IMEI number. This is accomplished by the system server changing portions of the ticket payload so that it is customized for each individual IMEI number associated with a ticket token. The animation code comprising the ticket payload is designed so that it has to obtain the correct IMEI number at run time. In another embodiment, at run-time, the animation code will read the particular ticket token specific for the phone that instance of the animation was transmitted to. The code will then decode the token and check that it reflects the correct IMEI number for that device.

6

In another embodiment, the security protocol first requires the user to login to the server with a login username and password. The application also transmits the IMEI, UDID or serial number of the device or any combination of them.

When verified by the server, an authorization key (Authkey) is transmitted to the device. The Authkey is a random number. When the user's application transmits a request for a validating visual object, it transmits the Authkey and the IMEI, UDID or serial number (or combination) that is used for verification. This is checked by the server for validity in the database. On verification, the validating visual object is encrypted using the Authkey and transmitted to the device. The application running on the device then uses the Authkey to decrypt and display the validating visual object. The Authkey is a one-time key. It is used once for each ticket payload. If a user buys a second ticket from the system, a different, second Authkey is associated with that second ticket payload. In one embodiment, the Authkey is unique to the ticket for a given event. In another embodiment, the Authkey is unique to the ticket, device and the event. In other embodiments, the Authkey can be replaced with a key-pair in an asymmetric encryption system. In that case, the validating visual object is encrypted with a "public" key, and then each user is issued a private key as the "Authkey" to be used to decrypt the object.

In yet another embodiment, the Authkey can be encrypted on the server and transmitted to the device in encrypted form. Only when the application is operating can the Authkey be decrypted with the appropriate key. In yet another embodiment, the application that displays the validating visual object can request a PIN number or some other login password from the user, such that if the device is lost, the tickets cannot be used by someone who finds the device.

In another embodiment, the application running on the device can fetch a dynamic script, meaning a piece of code that has instructions arranged in a different order for subsets of devices that request it. The ticket payload is then modified so as to have the same number of versions that are compatible with a corresponding variation in the dynamic script. As a result, it is difficult to reverse engineer the application because the application will be altered at run time and the ticket payload customized for that alteration. One embodiment of the dynamic script would be expressed in Java™ computer language and rendered using OpenView. The ticket payload can be an HTML file called using Ajax.

Security can also be enhanced by actively destroying the validating visual object so that it resides in the device for a limited time. In one embodiment, the ticket payload has a time to kill parameter that provides the application with a count-down time to destroy the validating visual object. In another embodiment, the validating visual object is displayed when the user holds down a literal or virtual button on the user interface of the device. When the button is released, the application destroys the validating visual object.

Security can also be enhanced by retaining as steganographic data embedded in the validating visual object, the IMEI, UDID, Serial number or phone number of the device. The application can be operated to recover that information and display it on the screen. This makes it possible for security personnel at a venue to view that information from a validly operating device. If the device is showing a pirated validating visual object, then the actual data associated with the device will not match and it will be apparent from inspection of the device. This way, suspicious ticket holders can be subject to increased scrutiny, the presence of which deters piracy.

In another embodiment, the ticket payload can operate a sound sampling application that requests the customer to

US 9,239,993 B2

7

speak in to the device. The application can then use that data to check whether the voice print of the speaker matches the expected voice print. In yet another embodiment, the device can take a picture of the customer's face, and then facial recognition code embedded in the ticket payload can operate to check whether the features of the face sufficiently match a pre-determined set of features, that is, of the customer's face at the time the ticket was purchased. In yet another embodiment, the verification can be supplemented by being sure that the use of the ticket is during a pre-determined period of time. In yet another embodiment, the verification can be supplemented by the ticket payload operating to check that the location of the venue where the ticket is being used is within a pre-determined range of tolerance to a GPS (Global Positioning System) location. In yet another embodiment, after a certain pre-determined number of downloads of ticket payloads for a specific show, the validating visual object is automatically changed. This last mechanism may be used for promotions, to select the first set of ticket buyers for special treatment at the venue. In yet another embodiment, two different validating visual objects may be used, which are selected based on the verified age of the customer. In this way, a venue can use the system to not only to verify ticket holders coming into the venue, but to verify their drinking age when alcoholic drinks are ordered.

In yet another embodiment, the system's servers control the ticket activation process. FIG. 12. In this embodiment, the token is generated randomly by the user's mobile computing device and then transmitted to and stored on the system server as a result of the user's request to activate the ticket. When the server receives a request to activate a ticket, the server checks whether there is already an activation token stored in its database that corresponds to that ticket. The token is stored in a data record associated with the user that is activating the ticket. The user logs into the account and then requests that a ticket be activated. If it is, then it checks whether the token received from the user's mobile device matches the stored token. That is, it authenticates against that stored token. If the user's request for activation is the first activation of the ticket, then the server stores the received token into the data record associated with the user's account and keeps it there for a predetermined period of time, in order to lock the ticket to that device for that period of time. This process locks a ticket to that unique token for that lock period. Typically this will lock the ticket to the user's mobile computing device. If the stored token does not match the token received from the user's computing device, the ticket activation is denied.

The predetermined lock time permits a reusable ticket to be locked to a device for the predetermined lock time. This is useful in the event the user changes the mobile computing device that the user uses to the ticket. For example, a monthly train commuting ticket would be activated once each day, and would remain activated for the day of its activation. In this case, the user would validate the ticket once each day, and that activation would be locked to the device for the day. The next day, the user would be able to activate the ticket using a different mobile computing device if the predetermined time locking the activation has expired, that is, if the data record associated with the ticket has been automatically reset into an deactivated state. The activation process also permits a user account to be shared within a family, for instance, but that each ticket sold to that account to be locked to one device.

As depicted in the protocol diagrams FIGS. 13a and 13b, the user can use their mobile computing device to request that their ticket get activated for the first time. However, once that activation process has occurred, the server will store the unique token received from the activating user's computing

8

device in the database in a manner that associates it with the ticket and the user's account. If another user associated with the account attempts to use the ticket by activating it, a different random token will be transmitted to the server. Because these two tokens do not match, the second activation will be prohibited.

The activation process can also permit a ticket to be shared. In this embodiment, the user who has activated the ticket can submit to the server a request that the ticket be transferred to another user. For example, a data message can be transmitted from the user's device to the system that embodies a request to move the ticket to another user. In that case, the stored token is marked as blocked, or is equivalently considered not present. This is accomplished by storing a data flag in the database that corresponds to the ticket. One logic state encodes normal use and the opposite logic state encodes that the ticket has been shared. A data message may be transmitted to the second user indicating that the ticket is available for activation. The second user may submit a request to activate the ticket and a random token value is transmitted from the second user's device to the server. That second token value is checked to see if it's the first activation. Because the first user has activated the ticket, but then transferred it, the activation by the second user is not blocked. That is, the server detects that the first token is now cancelled or equivalently, the system has returned to the state where the first activation has not occurred and therefore permits the new activation to take place. The new activation can also have a predetermined time to live value stored in the database that is associated with it. In this case, the activation by the second user expires and the second user can be prevented from reactivating the ticket. At the same time, the flag setting that disables the first token can be reset, thereby setting the ticket up for reactivation by the first user. By this mechanism, it is possible for the electronic ticket to be lent from one user to another.

In yet another embodiment, the ticket activation process can open a persistent connection channel over the data network that links the server and the user's mobile computing device. In this embodiment, if the activation of the ticket and therefore the device is successful, the server can maintain a persistent data channel with a computer process running on the user's computing device. In this embodiment, the request for ticket activation causes the user computer device to open the persistent channel. In this embodiment, the server establishes a communication process operating on the server that receives data and then causes that data to be automatically routed to the user's computing device. The process on the user's mobile computing device can thereby automatically respond to that received data. In tandem, the computer process operating on the users computing device can send data directly to the server process associated with that user's session. For a server servicing many user devices, there will be one persistent channel established between the server and each mobile device that has an activated ticket.

The persistent channel between the server and the user's computer device can be used in a variety of ways. In the preferred embodiment, the persistent connection is designed so that that it maintains a bi-directional, full-duplex communications channel over a single TCP connection. The protocol provides a standardized way for the server to send content to the process operating on the user's computing device without being solicited by the user's device each time for that information, and allowing for messages to be passed back and forth while keeping the connection open. In this way a two-way (bi-direction) ongoing interaction can take place between a process operating on the user's computing device the server. By means of the persistent channel, the server can

US 9,239,993 B2

9

control the activity of the user computer device. For each user computing device, there can be a distinct persistent connection.

In one embodiment, the persistent connection is established when the user requests an activation of a ticket. See FIG. 14. In other embodiments, it can be used if the system is used to verify payment of a purchase price. In either case, the user computing device transmits a request message to the server. For each user computing device, there can be a distinct persistent channel. Each persistent channel has a label or channel name that can be used by the server to address the channel. In the case of ticketing, when the ticket is activated the data representing the validating visual object can be transmitted in real time from the server to the user computing device and immediately displayed on the device. This provides an additional method of securing the visual ticketing process. In this case, when the ticket is activated and the persistent channel is created, the label of the channel is stored in the database in a data record associated with the user and the ticket. When the server transmits the validating visual object for that ticket, it fetches from the database the label of the channel and then uses that label to route the transmission of the validating visual object. The use of the persistent channel causes the user computer device to immediately and automatically act on the validating visual object. In one embodiment, the receipt of the validating visual object causes the receiving process to immediately in response interpret the command and select and display the required visual pattern. In another embodiment, the process receives a block of code that the process calls on to execute, and that code causes the visual pattern to be displayed. In yet another embodiment, the process receives image or video data and the process passes that data on to the user device screen display functions for presentation on the user device screen.

In another embodiment, a validating visual object can be transmitted to the user's computing device to be automatically displayed on the screen without the user having to input a command to cause the display. That visual object can be displayed by the user computing device. For additional security, the server can transmit to the user computing device a visual object that contains the channel name or a unique number that the server can map to the channel name. For clarity, this additional visual object is not necessarily used for visual verification by ticket takers, as explained above. This visual object can be used by other machinery to confirm the ticket purchase transaction or even other transactions not directly related to the purchase of the ticket. The additional visual object can be in the form of a QR code, barcode or any other visual object that can be scanned, for example at a point of sale system, and from that scanned image, an embedded data payload extracted. In that visual object, data can be embedded that uniquely identifies the source of the scanned object. The channel name of the persistent channel or a number uniquely mapped on the server to identify the channel can be embedded in that scanned object.

In one embodiment, as shown on FIG. 15, a merchant can use a point of sale system operated by the merchant to scan the display screen of the user's computing device. That point of sale system can then capture from the scanned image the channel name or a unique number that is uniquely mapped on the server to the channel name. That information is transmitted to the server as a challenge for verification. The received challenge data is checked to see if it matches the channel name or corresponding unique number used to transmit the visual object that the merchant scanned. If they match up, there is a verification of a transaction. This exchange provides

10

verification that the user's device is present at the merchant location and that a transaction with the merchant should be paid for.

In yet another embodiment, the persistent connection provides a means for the server to control the actions of the process operating on the user's computer device that is at the other end of the connection. In this embodiment, the server can automatically transmit a command to the process on the user's computing device that automatically deletes the verifying visual object that has been transmitted to ensure that it cannot be reused or copied.

In one embodiment, the persistent connection is used to automatically transmit visual information to the user's mobile computing device and to cause that information to be displayed on the screen of the device. The visual information can be the validating visual object or any other visual object that the server selects to transmit for display. In this embodiment, the persistent connection can be used by the server to transmit other information to the user's device. In this embodiment, the server transmits text, images, video or sound and in some cases in combination with other HTML data. In another embodiment, this material comprises advertising that the server selects to display on the user's device. The selection process can utilize the GPS feature described above to determine the approximate location of the user's device and then based on that location, select advertising appropriate to be transmitted to that device. In yet another embodiment, the server selects the advertising content by determining predetermined features of the validated ticket or purchasing transaction and then making a selection on the basis of those features. For example, a validation of a ticket to a baseball game played by a team specified in the data associated with the validated ticket may cause the selection of an offer to purchase a ticket for the next baseball game of the same team. In yet another embodiment, the character of the transaction being verified can be used to cause the selection of advertising or the transmission of data comprising a discount offer related to the transaction.

In this embodiment, the server receives from the merchant the data that determines the persistent channel. The merchant, by relying on the system for payment will also transmit transaction details, for example, an amount of money and an identity of goods or services. When the channel name or unique number associated with the channel is matched for verification, the server can transmit data representing a confirmation display down to the user's device using the persistent connection. This data is received by the user computing device and then automatically rendered by the process at the other end of the channel connection. In addition, the server can use the transaction information to determine one or more advertisements or discount offers to transmit to the user's computing device. The selection method can consist of one or more heuristics. In one example, the validation of the ticket for a baseball game can trigger the display of advertising for food or drinks. Likewise, a transaction for purchasing a cup of coffee can trigger an advertisement for purchasing a newspaper.

Operating Environment:

The system operates on one or more computers, typically one or more file servers connected to the Internet. The system is typically comprised of a central server that is connected by a data network to a user's computer. The central server may be comprised of one or more computers connected to one or more mass storage devices. A website is a central server that is connected to the Internet. The typical website has one or more files, referred to as web-pages, that are transmitted to a user's computer so that the user's computer displays an inter-

US 9,239,993 B2

11

face in dependence on the contents of the web-page file. The web-page file can contain HTML or other data that is rendered by a program operating on the user's computer. That program, referred to as a browser, permits the user to actuate virtual buttons or controls that are displayed by the browser and to input alphanumeric data. The browser operating on the user's computer then transmits values associated with the buttons or other controls and any input alphanumeric strings to the website. The website then processes these inputs, in some cases transmitting back to the user's computer additional data that is displayed by the browser. The precise architecture of the central server does not limit the claimed invention. In addition, the data network may operate with several levels, such that the user's computer is connected through a fire wall to one server, which routes communications to another server that executes the disclosed methods. The precise details of the data network architecture does not limit the claimed invention. Further, the user's computer may be a laptop or desktop type of personal computer. It can also be a cell phone, smart phone or other handheld device. The precise form factor of the user's computer does not limit the claimed invention. In one embodiment, the user's computer is omitted, and instead a separate computing functionality provided that works with the central server. This may be housed in the central server or operatively connected to it. In this case, an operator can take a telephone call from a customer and input into the computing system the customer's data in accordance with the disclosed method. Further, the customer may receive from and transmit data to the central server by means of the Internet, whereby the customer accesses an account using an Internet web-browser and browser displays an interactive webpage operatively connected to the central server. The central server transmits and receives data in response to data and commands transmitted from the browser in response to the customer's actuation of the browser user interface.

A server may be a computer comprised of a central processing unit with a mass storage device and a network connection. In addition a server can include multiple of such computers connected together with a data network or other data transfer connection, or, multiple computers on a network with network accessed storage, in a manner that provides such functionality as a group. Practitioners of ordinary skill will recognize that functions that are accomplished on one server may be partitioned and accomplished on multiple servers that are operatively connected by a computer network by means of appropriate inter process communication. In addition, the access of the website can be by means of an Internet browser accessing a secure or public page or by means of a client program running on a local computer that is connected over a computer network to the server. A data message and data upload or download can be delivered over the Internet using typical protocols, including TCP/IP, HTTP, SMTP, RPC, FTP or other kinds of data communication protocols that permit processes running on two remote computers to exchange information by means of digital network communication. As a result a data message can be a data packet transmitted from or received by a computer containing a destination network address, a destination process or application identifier, and data values that can be parsed at the destination computer located at the destination network address by the destination application in order that the relevant data values are extracted and used by the destination application.

It should be noted that the flow diagrams are used herein to demonstrate various aspects of the invention, and should not be construed to limit the present invention to any particular logic flow or logic implementation. The described logic may

12

be partitioned into different logic blocks (e.g., programs, modules, functions, or subroutines) without changing the overall results or otherwise departing from the true scope of the invention. Oftentimes, logic elements may be added, modified, omitted, performed in a different order, or implemented using different logic constructs (e.g., logic gates, looping primitives, conditional logic, and other logic constructs) without changing the overall results or otherwise departing from the true scope of the invention.

The method described herein can be executed on a computer system, generally comprised of a central processing unit (CPU) that is operatively connected to a memory device, data input and output circuitry (10) and computer data network communication circuitry. Computer code executed by the CPU can take data received by the data communication circuitry and store it in the memory device. In addition, the CPU can take data from the I/O circuitry and store it in the memory device. Further, the CPU can take data from a memory device and output it through the IO circuitry or the data communication circuitry. The data stored in memory may be further recalled from the memory device, further processed or modified by the CPU in the manner described herein and restored in the same memory device or a different memory device operatively connected to the CPU including by means of the data network circuitry. The memory device can be any kind of data storage circuit or magnetic storage or optical device, including a hard disk, optical disk or solid state memory.

Examples of well known computing systems, environments, and/or configurations that may be suitable for use with the invention include, but are not limited to, personal computers, server computers, hand-held, laptop or mobile computer or communications devices such as cell phones and PDA's, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputers, mainframe computers, distributed computing environments that include any of the above systems or devices, and the like.

Computer program logic implementing all or part of the functionality previously described herein may be embodied in various forms, including, but in no way limited to, a source code form, a computer executable form, and various intermediate forms (e.g., forms generated by an assembler, compiler, linker, or locator.) Source code may include a series of computer program instructions implemented in any of various programming languages (e.g., an object code, an assembly language, or a high-level language such as FORTRAN, C, C++, JAVA, or HTML) for use with various operating systems or operating environments. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (e.g., via an interpreter), or the source code may be converted (e.g., via a translator, assembler, or compiler) into a computer executable form.

The invention may be described in the general context of computer-executable instructions, such as program modules, being executed by a computer. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types. The computer program and data may be fixed in any form (e.g., source code form, computer executable form, or an intermediate form) either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (e.g., a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (e.g., a diskette or fixed hard disk), an optical memory device (e.g., a CD-ROM or DVD), a PC card (e.g., PCMCIA card), or other memory device. The computer pro-

US 9,239,993 B2

13

gram and data may be fixed in any form in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies, networking technologies, and inter-networking technologies. The computer program and data may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (e.g., shrink wrapped software or a magnetic tape), preloaded with a computer system (e.g., on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (e.g., the Internet or World Wide Web.) It is appreciated that any of the software components of the present invention may, if desired, be implemented in ROM (read-only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques.

The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote computer storage media including memory storage devices. Practitioners of ordinary skill will recognize that the invention may be executed on one or more computer processors that are linked using a data network, including, for example, the Internet. In another embodiment, different steps of the process can be executed by one or more computers and storage devices geographically separated by connected by a data network in a manner so that they operate together to execute the process steps. In one embodiment, a user's computer can run an application that causes the user's computer to transmit a stream of one or more data packets across a data network to a second computer, referred to here as a server. The server, in turn, may be connected to one or more mass data storage devices where the database is stored. The server can execute a program that receives the transmitted packet and interpret the transmitted data packets in order to extract database query information. The server can then execute the remaining steps of the invention by means of accessing the mass storage devices to derive the desired result of the query. Alternatively, the server can transmit the query information to another computer that is connected to the mass storage devices, and that computer can execute the invention to derive the desired result. The result can then be transmitted back to the user's computer by means of another stream of one or more data packets appropriately addressed to the user's computer.

The described embodiments of the invention are intended to be exemplary and numerous variations and modifications will be apparent to those skilled in the art. All such variations and modifications are intended to be within the scope of the present invention as defined in the appended claims. Although the present invention has been described and illustrated in detail, it is to be clearly understood that the same is by way of illustration and example only, and is not to be taken by way of limitation. It is appreciated that various features of the invention which are, for clarity, described in the context of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable combination. It is appreciated that the particular embodiment described in the specification is intended only to provide an extremely detailed disclosure of the present invention and is not intended to be limiting.

Modifications of the above disclosed apparatus and methods which fall within the scope of the invention will be readily

14

apparent to those of ordinary skill in the art. Accordingly, while the present invention has been disclosed in connection with exemplary embodiments thereof, it should be understood that other embodiments may fall within the spirit and scope of the invention, as defined by the following claims.

What is claimed:

1. A method performed by a computer system for displaying visual validation of the possession of a previously purchased electronic ticket for utilization of a service monitored by a ticket taker comprising:

transmitting a token associated with a previously purchased electronic ticket to a remote display device, wherein the token is a unique alphanumeric string, and wherein a copy of the unique alphanumeric string is stored on a central computer system;

validating the token by matching the token transmitted to the remote display device to the copy of the unique alphanumeric string stored on the central computing system to provide a ticket payload to the remote display device;

securing a validation display object prior to transmission to provide a secured validation display object;

transmitting to the remote display device a secured validation display object associated with the ticket payload; and

enabling the remote display device to display the secured validation display object upon validation of the token for visual recognition by the ticket taker or preventing the remote display device from displaying the secured validation display object in the event that the token is not validated.

2. The method of claim 1 further comprising:

receiving from the remote display device a request to verify the purchase of the previously purchased electronic ticket;

determining the validity of the received request; and transmitting a response to the remote display device confirming the verification of the previously purchased electronic ticket by displaying the secured validation display object on the remote display device.

3. The method of claim 2 further comprising:

transmitting the validation display object to the remote display device prior to receiving the request for verification.

4. The method of claim 3 further comprising:

securing the validation display object prior to transmission of the validation display object against being displayed on the remote display device when the previously purchased electronic ticket has not been verified.

5. The method of claim 4 wherein the securing step is comprised of:

encrypting the validation display object.

6. The method of claim 1 further comprising:

transmitting security data to the remote display device to authenticate the secured validation display object.

7. The method of claim 1 where the securing step is comprised of:

encrypting the secured validation display object.

8. A system for validating previously purchased electronic tickets for utilization of a service monitored by a ticket taker, comprising:

a central computer system and

at least one remote display device operatively connected to the central computer system over a data communication network,

US 9,239,993 B2

15

wherein the central computer system:

transmits a token associated with the previously purchased electronic ticket to the at least one remote display device,

wherein the token is a unique alphanumeric string, and wherein a copy of the unique alphanumeric string is stored on the central computer system; and

upon a request received in the at least one remote display device, validates the token associated with the previously purchased electronic ticket by matching the token transmitted to the remote display device to the copy of the unique alphanumeric string stored on the central computing system to provide a ticket payload to the at least one remote display device;

secures a validation display object prior to transmission to provide a secured validation display object;

transmits to the remote display device over the data communication network the secured validation display object associated with the ticket payload, and

wherein the remote display device:

enables display of the secured validating display object upon validation of the token for visual recognition by the ticket taker or prevents the remote display device from displaying the secured validation display object in the event that the token is not validated.

9. The system of claim 8 wherein the secured validation display object is not displayable without verification of the previously purchased electronic ticket.

10. The system of claim 9 wherein the secured validation display object is secured by encryption means.

11. The system of claim 9 wherein the remote display device receives and stores the secured validation display object prior to verification of the purchase of the previously purchased electronic ticket.

12. The system of claim 11 wherein the remote display device is further configured to display the secured validating display object without a network connection with the central computer system.

13. The system of claim 8 wherein the remote display device displays the secured validating display object without a network connection with the central computer system.

14. The system of claim 13 wherein the secured validation display object is further comprised of data parameters that are configured to be used by the remote display device to perform the purchase validation.

16

15. The system of claim 8 wherein the secured validation display object is further configured to change based on a user of the remote display device actuating the user interface of the remote display device in a predetermined manner.

16. The system of claim 15 wherein the predetermined manner of actuation is the user touching a predefined area of a display screen on the remote display device.

17. The system of claim 16 wherein the predefined area of the display screen appears as a button.

18. The system of claim 8 wherein the predetermined manner of actuation is the input of a code into the remote display device by the user.

19. The system of claim 15 wherein the predetermined manner of actuation is the input of a sound into the remote display device.

20. The system of claim 15 wherein the predetermined manner of actuation is the detection of a predetermined location by means of a GPS detector incorporated within or attached to the remote display device.

21. The system of claim 15 wherein the predetermined manner of actuation is input of a predetermined visual image.

22. The system of claim 8 wherein the secured validation display object is further configured to display in different versions of appearance where the selection of version is dependent on a pre-determined schedule.

23. The system of claim 8 wherein the central computer system transmits the secured validating display object to the remote display device in dependence on completion of a purchase of the previously purchased electronic ticket.

24. The system of claim 8 wherein the secured validation display object is configured to be unique to a specific remote display device it is intended to be displayed on.

25. The system of claim 8 wherein the data communication network is configured to have a persistent channel between the central computer system and the remote display device through which the central computer system can push content.

26. The system of claim 25 wherein the content is an advertisement that is selected from a plurality of advertisements in dependence on the type of purchased electronic ticket.

* * * * *

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

BYTEMARK, INC.

§

§

v.

§

Case No. 2:16-cv-00543-JRG-RSP

§

MASABI LTD.

§

REPORT AND RECOMMENDATION

On May 20, 2016, Bytemark filed a lawsuit against Masabi, alleging that Masabi infringes claims of U.S. Patent Nos. 8,494,967 and 9,239,993. *See* Compl., Dkt. 1. Bytemark is now asserting claims 1-5, 17-22, and 34 of the '967 patent, and claims 1-17, and 22-24 of the '993 patent. Dkt. 112-7 at 1. Masabi has moved for summary judgment of invalidity, contending that the asserted claims are invalid under 35 U.S.C. §§ 101, 102, 103, and 112. Dkt. 113. Plaintiff has filed a lengthy response. Dkt. 121. Because the claims recite subject matter that is not patent-eligible, the Court recommends that summary judgment of invalidity under § 101 be granted, that summary judgment of invalidity on the other grounds be denied as moot, and that the stay previously entered be lifted.

BACKGROUND

The '967 and '993 patents generally relate to computer systems and methods for verifying the authenticity of an electronic ticket. The patents trace back to two applications filed in March 2011. The patents are also related to a common parent application filed on May 18, 2012. The parent application claims priority to an application filed on March 11, 2011. The application leading to the '993 patent is a continuation of the application that became the '967 patent, and, consequently, both patents-in-suit share a nearly identical specification.

The problem described by the patents relates to authenticating a previously purchased electronic ticket displayed on a customer's phone or mobile device. *See* '967 patent at 1:24-43. According to the patents "[v]enues such as theaters, amusement parks and other facilities that use tickets, for example airlines, ferries and other transportation have a need to use electronic ticketing." *Id.* at 1:24-26. Electronic ticketing systems existed, but verifying the authenticity of the ticket was difficult. *Id.* at 1:28. An electronic ticket that included a barcode, for example, could be displayed on a customer's mobile phone, but the phone had to be placed on a scanner that reads the barcode. *Id.* at 1:30-32. The problem with this process, as the patents describe it, is that it "is fraught with error and the time taken to verify the electronic ticket far exceeds that of the old system: looking at the paper ticket and tearing it in half." *Id.* at 1:32-35. This is because barcode scanners were not designed to read an LCD screen displaying a barcode. *Id.* at 1:35-36. The patents describe a "need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket." *Id.* at 1:38-40.

The patents describe the invention as a "novel system and method for distributing electronic ticketing such that the ticket is verified at the entrance to venues by means of an animation or other human perceptible verifying visual object that is selected by the venue for the specific event." *Id.*, abstract. The verifying visual object "removes the need to use a bar-code scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders." *Id.*

The '967 patent includes three independent claims, all of which recite similar methods and systems for implementing the ticket-authentication process. Claim 1 recites:

A method by a server system for obtaining visual validation of the possession of a purchased electronic ticket on a user's computer device for presentation to a ticket taker comprising:

receiving from the user's computer device a request to verify purchase of a previously purchased electronic ticket and to obtain a visual validation display object that confirms that the user possesses the previously purchased electronic ticket for utilization of a service monitored by the ticket taker, the visual validation display object configured to be readily recognizable visually by the ticket taker;

receiving from the user's computer device a token associated with the received request;

determining whether a token associated with the purchased electronic ticket has been stored in a data record associated with the received request, and if it has, whether the received token is valid; and

in dependence on the determination that the received token is valid, causing an activation of the purchased electronic ticket by transmitting to the user's computer device a data file comprising the visual validation display object that causes upon visual recognition by the ticket taker, the user to be permitted to utilize the service monitored by the ticket taker.

The asserted claims that depend from claim 1 (claims 2-5) recite additional steps, such as encrypting the visual validation object using an authorization key, as recited in claim 5, for example. Independent claim 17 recites a system capable of performing the method recited in claim 1, with the only meaningful difference being that claim 17's preamble specifies that the system is "[a] non-transitory computer readable data storage medium containing computer code" capable of executing instructions. Claim 17 has no dependent claims. Independent claim 18 recites a nearly identical system to that recited in claim 17, "configured to perform" the method of ticket authentication, and the asserted claims that depend from claim 18 recite limitations similar to those in the other dependent claims.

The only notable difference in the '993 patent claims is that the '993 patent claims are in one respect narrower than the claims of the '967 patent. Namely, the '993 patent claims recite that the "token" is "a unique alphanumeric string." This limitation appears in both independent claims

(claims 1 and 8). The claims are otherwise not meaningfully different than the '967 patent claims.

Claim 1 of the '993 patent, for example, recites:

A method performed by a computer system for displaying visual validation of the possession of a previously purchased electronic ticket for utilization of a service monitored by a ticket taker comprising:

transmitting a token associated with a previously purchased electronic ticket to a remote display device, wherein the token is a unique alphanumeric string, and wherein a copy of the unique alphanumeric string is stored on a central computer system;

validating the token by matching the token transmitted to the remote display device to the copy of the unique alphanumeric string stored on the central computing system to provide a ticket payload to the remote display device;

securing a validation display object prior to transmission to provide a secured validation display object;

transmitting to the remote display device a secured validation display object associated with the ticket payload; and

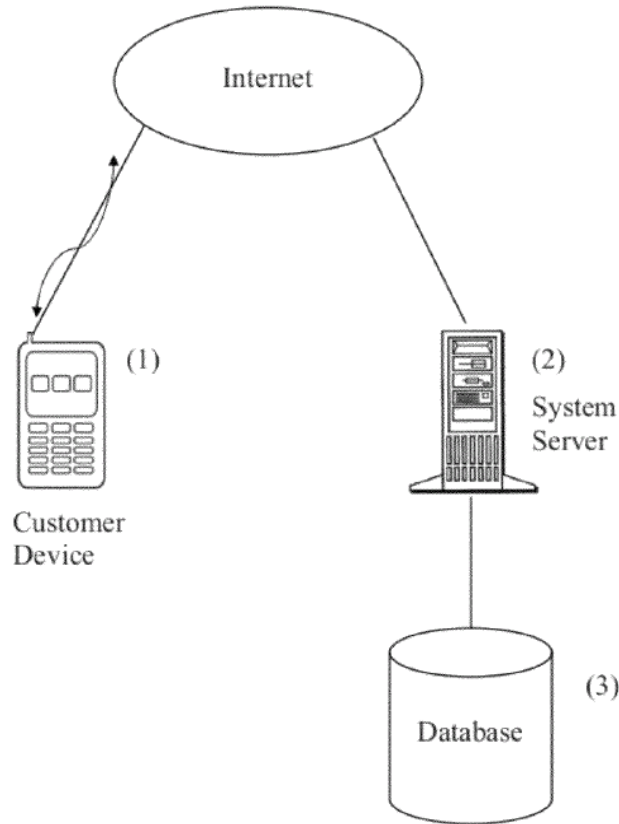
enabling the remote display device to display the secured validation display object upon validation of the token for visual recognition by the ticket taker or preventing the remote display device from displaying the secured validation display object in the event that the token is not validated.

The claims that depend from claims 1 and 8 of the '993 patent, like the dependent claims of the '967 patent, recite additional steps, but the essence of the invention is captured by the independent claims.

I. The Claims' Software, Data, and Hardware Elements

The asserted claims recite, with varying terminology, two hardware elements: a computer or server system and a customer's device. The specification refers to the computer system or server primarily in terms of its function. As shown in Figure 1 of the '967 patent, for example, the website where the customer purchases an electronic ticket accesses a server system, which is coupled to a

database that includes information related to the venue, the customer's username and password, and other information. '967 patent at Fig. 1, 3:41-60.

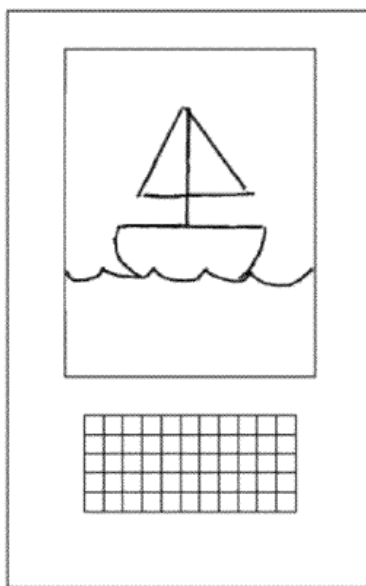


When the user selects a ticket, the user can also select a visual validating object. *Id.* at 3:41-60. The server then transmits the selected object to the customer's device. *See, e.g., id.* at 2:42-44. The server also generates and sends the token to the customer's device. *Id.* at 5:48-50.

The server is otherwise described as a website or file server connected to the internet and a database. *See, e.g., id.* at 10:52-11:28, 2:4-5. The central server, for example, can be "a computer comprised of a central processing unit with a mass storage device and a network connection." *Id.* at 11:29-56. Notably, "[t]he precise architecture of the central server does not limit the claimed invention." *Id.* at 11:4-6.

Similarly, the “computer device” or “remote display device” recited in the claims is described in broad, generic terms. The precise definition of these terms is difficult to determine because the terminology used even within the same patent is often inconsistent. The specification of ’967 patent, for example, equates “servers” with “one or more computers,” and the term “computer device” is not clearly defined. *See id.* at 2:4-6. The specification does state, however, that “[a] customer’s device can be a personal computer, mobile phone, mobile handheld device like a Blackberry or iPhone or any other kind of computing device a user can use to send and receive data messages.” *Id.* at 2:6-9. Such devices, as the specification acknowledges, are “well known computing systems.” *Id.* at 12:21-30. The purpose of the computer device is to receive the visual validating object and token and display the validating object on the screen of the device so that a ticket taker can verify the authenticity of the ticket. *See id.* at 2:10-11.

In addition to the hardware elements, the asserted claims generally include three software or data elements: the “validation display object,” the “token,” and the “electronic ticket.” The “visual validation display object” is a unique image. “The criterion for what constitutes a validating visual object is one that is readily recognizable from human observation” and which is “encapsulated in such a way as to be transmitted to the customer’s device with a minimum of network latency or download time, and that can be reasonably secured so as to avoid piracy.” ’967 patent at 3:12:23. The parties disputed the meaning of “visual validation display object” and “validation display object” during claim construction, and the Court resolved the dispute by construing these terms to mean “any object that is readily recognizable from human observation that can verify a ticket, or the code or commands that can generate such an object.” Dkt. 81 at 11. An example of a visual validation display object is a sailboat, as shown in Figure 5 of the ’967 patent:



The other two software or data elements are also stored on the server and ultimately transmitted to the customer's device. The "token" recited in the claims is "a unique number." '967 patent at 2:45-48. The token can be generated, for example, by the website where a customer purchases a ticket. *Id.* The website then sends the token to the user's device. *Id.* The claims of the '993 patent further specify that the token "is a unique alphanumeric string." *See, e.g.,* '993 patent, claim 1. The term "electronic ticket" is not defined by the patent, implying that the claimed electronic ticket is the same as those that existed in the prior art discussed in the specification. *See, e.g.,* '967 patent at 1:27-46.

II. Prosecution of the Patents-in-Suit and Related Applications

The prosecution history of the application that ultimately became the '967 patent contains one noteworthy rejection. Claims 1-16, as originally filed, recited methods similar to those that ultimately appeared in the issued claims. Original claims 17 and 18 were directed to systems for performing the method recited in claim 1. Claim 17 recited "[a] system comprised of a website adapted to perform any of the methods of Claims 1-16," while claim 18 recited "[a] computer

readable medium containing computer program code that when run causes the performance of any of the methods of Claims 1-16.” In an office action dated September 28, 2012, the examiner rejected these claims under § 101 because the claims were “directed to non-statutory subject matter.” Office Action, Appl. No. 13/475,881, at 3 (Sept. 28, 2012). Both claims, according to the examiner, were directed only to software or transitory signals, both of which constituted ineligible subject matter under existing Patent Office guidelines. The applicant overcame this rejection by amending the claims to recite hardware components and a “non-transitory” computer-readable medium. *See Resp.*, Appl. No. 13/475,881 (Mar. 27, 2013). The examiner allowed the claims on April 10, 2013, more than a year before the Supreme Court decided *Alice Corp. Pty v. CLS Bank Int’l*, 134 S. Ct. 2347 (2014).

The application leading to the ’993 patent did not escape the § 101 challenge as easily. The first rejection of the ’993 application came about six months after *Alice*. Although the examiner did not cite *Alice*, the *Alice* test was the basis for one of the rejections. The examiner regarded all the pending claims as being directed to the abstract idea “of organizing human activity such as purchasing a ticket and then showing a ticket to access either goods or services.” Office Action, Appl. No. 13/901,243, at 3 (Oct. 29, 2014). The additional claim elements, according to the examiner, were “mere instructions to implement the idea on a computer” or “well-understood, routine, and conventional activities previously known to the pertinent industry.” *See id.*

The applicant’s first attempt at responding to this rejection was not successful. The applicant argued that the “validation display object” has certain properties and is “readily recognizable visually,” and that this feature renders the claims patent-eligible. *See Office Action*, Appl. No. 13/901,243, at 2 (May 27, 2015). This argument was not persuasive because, according to the examiner, the validation display object is no different than a physical ticket that is verified

visually by a ticket taker. *See id.* at 2-3. The applicant also argued that the invention “solves technological problems with computer technology (LCD screens, scanners)” inasmuch as the invention avoids the need for a barcode. *See id.* at 3-4. The examiner found this argument unpersuasive because while the specification discussed “the flaw in the present technology,” the specification did not reveal an “inventive step,” or an improvement to the technology itself. *See id.* at 4.

After the applicant filed a request for continued examination and paid the requisite fee, the examiner allowed the claims. In the notice of allowance, the examiner stated that “[t]he matter of judicial exception was discussed between the Examiner and a 101 expert, Jim Trammell.” Notice of Allowance, Appl. No. 13/901,243, at 2 (Sept. 9, 2015). During this discussion, the examiner and Mr. Trammell concluded that the claims represent a technological advance by “adding greater security to an electronic ticket.” *See id.* The claims issued on December 29, 2015.

Although the claims of the patents-in-suit eventually overcame scrutiny under then-existing interpretations of § 101 and *Alice*, a number of related applications remained in prosecution, and these applications have not fared as well. These applications have specifications that are similar to those of the patents-in-suit, and many of these claims are remarkably similar to those recited in the asserted patents. In April of 2017, the claims in one of these applications were rejected under § 101 as being “directed to abstract idea of determining fraudulent activity associated with a ticketing system.” *See* Office Action, Appl. No. 14/286,622, at 3 (Apr. 13, 2017). This idea, according to the examiner, was similar to the idea found abstract and patent-ineligible in *FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089 (Fed. Cir. 2016). *See id.* The additional elements recited in the those claims, including a “server computer sub-system,” a “device,” and a “network” were not significant enough, in the examiner’s view, to take the claims

away from the abstract idea. *See id.* Another examiner lodged the same rejection in a similar application, finding that the claims were directed to the abstract idea of “electronic ticket verification.” *See* Office Action, Appl. No. 14/597,905, at 3 (Oct. 6, 2017). According to this examiner, the claims were similar to claims directed to data recognition and storage, such as those found ineligible in *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass’n*, 776 F.3d 1343 (Fed. Cir. 2014). *See* Office Action, Appl. No. 14/823,157, at 4 (Oct. 6, 2017).

For much of the same reasons as the examiners have articulated in these related patent applications, Masabi argues that the asserted claims of the patents-in-suit cannot withstand scrutiny under current § 101 jurisprudence. Accordingly, Masabi moves for summary judgment that the asserted claims are invalid for failure to recite patent-eligible subject matter.

DISCUSSION

A patent may be obtained for “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof.” 35 U.S.C. § 101. The exception is that “[l]aws of nature, natural phenomena, and abstract ideas are not patentable.” *Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S.Ct. 2107, 2116 (2013) (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S.Ct. 1289, 1293 (2012)). In assessing subject-matter eligibility, a court must “first determine whether the claims at issue are directed to a patent-ineligible concept.” *Alice*, 134 S.Ct. at 2355. If the claims are directed to an ineligible concept, the court must then “consider the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Id.* (quoting *Mayo*, 132 S.Ct. at 1298, 1297).

I. The Asserted Claims Are Directed to an Abstract Idea

When evaluating claims related to computer technology, a court must “articulate with specificity what the claims are directed to, and ‘ask whether the claims are directed to an improvement to computer functionality versus being directed to an abstract idea.’” *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017) (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016)) (citing *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1347 (Fed. Cir. 2017)). At least four considerations help guide the step one inquiry: the claim language, the specification, the prosecuting history, and past cases. *See, e.g., OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359 (Fed. Cir.), *cert. denied*, 136 S. Ct. 701, 193 L. Ed. 2d 522 (2015). In addition, while patent eligibility under § 101 is an issue of law, the ultimate legal conclusion may require an underlying factual determination. *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1341 (Fed. Cir. 2013). The Court finds no relevant disputed underlying facts in this case, nor has Plaintiff demonstrated any.

The claim language often reveals whether an invention is directed to an improvement to computer technology, on the one hand, or merely the implementation of an abstract idea using computers, on the other. *Enfish*, 822 F.3d at 1336, 1339; *Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1348 (Fed. Cir. 2016). Computer-related claims withstanding scrutiny by the Federal Circuit under step one have generally recited a technological improvement in the claims themselves. *See Visual Memory*, 867 F.3d at 1259 (enhanced computer memory system); *Thales*, 850 F.3d at 1345 (motion-tracking system); *Enfish*, 822 F.3d at 1339 (self-referential table). In close cases, it may be difficult to determine what the claims are directed to under step one, and in such cases, the claim language may reveal concrete improvements to

computer technology under the step two analysis. *See Enfish*, 822 F.3d 1327 (Fed. Cir. 2016); *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257-59 (Fed. Cir. 2014).

This is not a close case under step one. The preambles of the asserted claims all refer to a method of authenticating a ticket by showing a ticket taker a validation display object. The claims recite the use of computers, servers, and devices, but these components are referenced in terms of their conventional functions, such as sending, receiving, storing, and verifying data or information. It is well established that “claims directed to the collection, storage, and recognition of data are directed to an abstract idea.” *Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, No. 2016-1233, 2017 WL 4654964, at *6 (Fed. Cir. Oct. 18, 2017). The features of the claims may enable a ticket taker to verify the authenticity of a ticket quickly and efficiently, but this is not an improvement to the technology itself. Federal Circuit precedent “is clear that merely adding computer functionality to increase the speed or efficiency of the process does not confer patent eligibility on an otherwise abstract idea.” *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1370 (Fed. Cir. 2015).

Similarly, the software or data elements recited in the claims are not technological improvements. Nor is the combination of those elements. The “validation display object” is simply an image, such as a sailboat, created by and stored on a computer. The “token” is a number, and the use of tokens, or “tokenization” was well-known long before the priority dates of the asserted claims. *See* Dkt. 113 at 15. Indeed, as the Federal Circuit recently found, the use of “tokens” in a computer environment is not a technological improvement, but rather “much like the identification of a coin or token as genuine in a mechanical transit system toll device.” *Smart Sys. Innovations*, 2017 WL 4654964, at *8. ” The “electronic ticket” is likewise not a technological improvement because the claims themselves contain no indication that the ticket is anything other than the type

of well-known electronic ticket described in the specification—without any reference to the technical details of the ticket. The absence of technical details indicating that a hardware or software component recited in the claims is a technological improvement supports a finding that the claims are abstract. *See id.* In sum, the patent-ineligible abstract idea “is plainly identifiable and divisible from the generic computer limitations recited by” the claims. *DDR Holdings*, 773 F.3d at 1256. Finally, although claim 1 of both patents is sufficiently representative, *see Content Extraction*, 776 F.3d at 1348, the dependent claim limitations do not alter the analysis.

The specification and prosecution history of a patent can also be useful in determining whether the claims are directed to an abstract idea. The specification will often emphasize the feature of the claims that distinguishes them from the prior art. In *Enfish*, for example, the specification disparaged conventional data structures and described the “present invention” as the self-referential table recited in the claims, which supported the Federal Circuit’s conclusion that the claims were patent-eligible. *See* 822 F.3d at 1339. By contrast, the specification and prosecution history in *OIP Technologies* emphasized that the “key distinguishing feature of the claims is the ability to automate or otherwise make more efficient traditional price-optimization methods.” *See* 788 F.3d at 1363.

The step one inquiry in this case could likely end with the claim language, but the specification and prosecution history support the conclusion that is evident from the claims. The background of the patents discusses the existing problem with electronic ticketing and the “need for an electronic ticketing system that provides a human-perceivable visual display that the venue can rely on to verify the ticket.” ’967 patent at 1:38-40. The patents describe the invention as a “novel system and method for distributing electronic ticketing such that the ticket is verified at the entrance to venues by means of an animation or other human perceptible verifying visual object

that is selected by the venue for the specific event.” *See, e.g., id.*, abstract. The verifying visual object “removes the need to use a bar-code scanner on an LCD display of a cell phone or other device and speeds up the rate at which human ticket takers can verify ticket holders,” *id.*, but there is no indication that the image itself or the method of creating it is a technological improvement, *cf. McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314 (Fed. Cir. 2016) (patent focused on “specific asserted improvement in computer animation”).

The prosecution history points to the same conclusion. First, the use of a validation display object was repeatedly emphasized as an important aspect of the invention. In distinguishing a prior art reference during the prosecution of the ’967 patent, for example, the applicant emphasized that the validation display object is “readily recognizable by a ticket taker, as in the form of an image, an animation or other dynamic object that permits the ticket taker to effortlessly and quickly recognize that the device is displaying an object that the ticket taker expects to see at that time.” Resp., Appl. No. 13/475,881, at 9 (Mar. 27, 2013).

Second, claims 17 and 18, as originally-filed, recited “[a] system comprised of a website adapted to perform any of the methods of Claims 1-16,” and “[a] computer readable medium containing computer program code that when run causes the performance of any of the methods of Claims 1-16,” respectively. While the inquiry must focus on the issued claims, the method recited in the original claims is not meaningfully different than the method recited in the claims that issued. By essentially reciting nothing more than “perform the method on a computer,” original claims 17 and 18 suggest that the focus of the invention is an abstract idea for which “for which computers are invoked merely as a tool.” *See Enfish*, 822 F.3d at 1336.

Third, the examiner rejected the ’993 patent claims under *Alice* well before its contours had been defined by the Federal Circuit. Bytemark emphasizes that the applicant overcame this

rejection, and that the examiner even made the rare decision to consult a “101 expert” before allowing the claims. But the Supreme Court had issued the *Alice* decision only six months before the claims were allowed, and the reach of *Alice* was not yet understood. Notably, in the continuation applications that remain pending today, claims that arguably include greater technical detail than the asserted claims have been rejected by the Patent Office under more recent § 101 precedent.

In addition to the claims, specification, and prosecution history, it is often “sufficient to compare claims at issue to those claims already found to be directed to an abstract idea in previous cases.” *See Enfish*, 822 F.3d at 1335. Claims that are similar to the claims at issue here were found to be directed to an abstract idea in *Smart Systems Innovations*. *See* 2017 WL 4654964. The claims involved “acquiring identification data from a bankcard, using the data to verify the validity of the bankcard, and denying access to a transit system if the bankcard is invalid.” *Id.* at *6. The point of the invention was to allow “riders to conveniently and quickly access mass transit by using existing bankcards.” *Id.* at *2. But the claims did not improve an existing technological process and were not, for example, directed to “a new type of bankcard, turnstile, or database.” *Id.* at *6. The Federal Circuit rejected the appellant’s argument that the claims are patent-eligible “because they improve prior systems of fare collection by speeding up the process at the turnstile.” *Id.* A district court invalidated similar claims directed to verifying and authenticating certain information, and minimizing tampering, during an online bingo game. *See Planet Bingo, LLC v. VKGS, LLC*, 961 F.Supp.2d 840 (W.D. Mich. 2013).

More generally, the claims are a hybrid of two categories of claims routinely invalidated under § 101. On one hand, the asserted claims involve collecting, storing, recognizing, and manipulating data, or encoding or decoding data, to make the data human- or machine-readable.

This feature of the claims has been repeatedly characterized as being directed to an abstract idea. *See Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1340-41 (Fed. Cir. 2017). On the other hand, the method recited in the asserted claims ensures the security of a financial transaction, and may improve the ticket-taking process. Claims directed to business practices or financial transactions are also routinely invalidated under § 101. *See id.* at 1340. Finally, the claims do not resemble claims directed to improved computer technology that have survived scrutiny under *Alice* step one. *See Visual Memory*, 867 F.3d at 1259 (enhanced computer memory system); *Thales*, 850 F.3d at 1345 (motion-tracking system); *Enfish*, 822 F.3d at 1339 (self-referential table). In sum, the claims are directed to the abstract idea of verifying the authenticity of a ticket.

II. The Claims Lack an Inventive Concept

It becomes apparent, in light of the step one analysis, that the asserted claims do not include an inventive concept sufficient to move the claims away from the abstract idea. A claim contains an inventive concept if it “include[s] additional features” that are more than “well-understood, routine, conventional activities.” *Alice*, 134 S.Ct. at 2357. Each hardware or software feature of the asserted claims is conventional, as is the manner in which those features operate and interact. The hardware features—a computer or server system and a mobile device—were both well known, and this is evident from the specification. The server is described in broad, almost unlimited terms, and, indeed, “does not limit the claimed invention.” *See, e.g.*, ’967 patent at 11:4-6. The mobile devices, as the specification acknowledges, were “well known computing systems.” *Id.* at 12:21-30. The same is true of the software and data components—the “validation display object,” the “token,” and the “electronic ticket.” There is no indication that any of these elements, or their combination, is the product of an inventive concept. Rather, the claims, specification, and

prosecution history all suggest that the concept recited in the claims is nothing more than using these conventional tools to verify the authenticity of an electronic ticket. *See, e.g.*, '967 patent, abstract; Resp., Appl. No. 13/475,881, at 9 (Mar. 27, 2013). When claims like the asserted claims are directed to an abstract idea, generic computer implementation does not move the claims "into section 101 eligibility territory." *See buySAFE Inc. v. Google, Inc.*, 765 F.3d 1350, 1354 (Fed. Cir. 2014).

The fact that the claims may be confined to a particular application, or that they may even be narrow, is not sufficient to change the analysis. Limiting an abstract idea "to a particular . . . environment does not render the claims any less abstract." *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1259 (Fed. Cir. 2016). A claim that is limited to a particular environment, or a narrow claim, may not preempt application of the abstract idea, but "[w]hile preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015), *cert. denied*, 136 S. Ct. 2511, 195 L. Ed. 2d 841 (2016). In other words, ineligibility may be most evident where a claim wholly preempts application of an idea, but the inverse is not necessarily true. A claim that does not preempt application of an idea may be ineligible simply because it recites ineligible subject matter as defined by *Alice* and its progeny, rendering the preemption inquiry moot. *Id.* Such is the case here.

CONCLUSION

The claims of the '967 and '993 patents may have improved the way ticket takers verify the authenticity of an electronic ticket. The claimed invention may have reduced long-lines and the prevalence of counterfeit tickets. And, as the prosecution history of the patents reveals, the claims at one time may have passed the § 101 filter. But under the law as it stands today, the

asserted claims are not patent-eligible. Accordingly, the Court recommends that Masabi's motion for summary judgment of invalidity under § 101 be granted, that the motion for summary judgment of invalidity on other grounds be denied as moot, and the stay previously entered be lifted.¹

SIGNED this 25th day of November, 2018.


ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE

¹ A party's failure to file written objections to the findings, conclusions, and recommendations contained in this report within fourteen days after being served with a copy shall bar that party from de novo review by the district judge of those findings, conclusions, and recommendations and, except on grounds of plain error, from appellate review of unobjected-to factual findings, and legal conclusions accepted and adopted by the district court. Fed. R. Civ. P. 72(b)(2); *see Douglass v. United Servs. Auto. Ass'n.*, 79 F.3d 1415, 1430 (5th Cir. 1996) (en banc).

**United States Court of Appeals
for the Federal Circuit**

CERTIFICATE OF SERVICE

I, Julian Hadiz, being duly sworn according to law and being over the age of 18, upon my oath depose and say that:

Counsel Press was retained by KEYHANI LLC, Attorneys for Plaintiff-Appellant to print this document. I am an employee of Counsel Press.

On **May 6, 2019**, Counsel for Appellant has authorized me to electronically file the foregoing **Brief for Plaintiff-Appellant** with the Clerk of Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF users:

Thomas Donahue
FISHERMAN STEWART PLLC
39533 Woodward Avenue, Suite 140
Bloomfield Hills, MI 48304
(248) 593-3303
tdonahue@fishstewip.com

Counsel for Defendant-Appellee

Upon request by the Court of the e-filed document, six paper copies will be filed with the Court within the time provided in the Court's rules.

Dated: May 6, 2019

/s/ Julian Hadiz
Counsel Press

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME
LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE
REQUIREMENTS**

1. This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) or Federal Rule of Appellate Procedure 28.1(e)

✓ The brief contains 12,410 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii), or

 The brief uses a monospaced typeface and contains lines of text, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) or Federal Rule of Appellate Procedure 28.1(e) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6)

✓ The brief has been prepared in a proportionally spaced typeface using Microsoft Word in a 14 point Times New Roman font or

 The brief has been prepared in a monospaced typeface using in a characters per inch font.

Dated: May 6, 2019

/s/ Dariush Keyhani
DARIUSH KEYHANI
KEYHANI LLC
1050 30th Street, NW
Washington, DC 20007
(202) 748-8950
dkeyhani@keyhanillc.com