

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DataDome S.A. and DataDome Solutions, Inc.,
Petitioner,

v.

Arkose Labs Holdings, Inc.,
Patent Owner.

U.S. Patent No. 9,148,427

Original Issue Date: September 29, 2015

Title: SYSTEM AND METHOD FOR IMPLEMENTING A ROBOT PROOF
WEB SITE

Case No. IPR2025-00694

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,148,427
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42 *et seq.***

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	37 C.F.R. § 42.8(B): MANDATORY NOTICES	4
A.	37 C.F.R. § 42.8(b)(1): Notice of Real Parties-in-Interest.....	4
B.	37 C.F.R. § 42.8(b)(2): Notice of Related Matters.....	4
C.	37 C.F.R. § 42.8(b)(3) and (4): Notice of Counsel and Service Information.....	5
D.	Fee for Inter Partes Review	5
III.	REQUIREMENTS FOR IPR.....	5
A.	§ 42.104(a): Grounds for Standing.....	6
B.	§ 42.104(b): Identification of Challenge	6
1.	§ 42.104(b)(1): Challenged Claims	6
2.	§ 42.104(b)(2): The Prior Art and Statutory Grounds	6
3.	Level of Ordinary Skill in the Art.....	9
4.	§ 42.104(b)(5): Evidence Supporting Challenge	9
IV.	INSTITUTION SHOULD BE GRANTED	10
A.	There Are No Grounds for a § 314 Discretionary Denial	10
B.	Denial Under § 325(d) Would Be Inappropriate.....	11
V.	TECHNOLOGY BACKGROUND.....	11
VI.	THERE EXISTS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE	13
A.	Problem Addressed by the '427 Patent and the Alleged Invention.....	14

B. Prosecution History	17
C. Claim Construction.....	20
VII. THE PRIOR ART.....	20
A. Lillibridge	20
B. Lim.....	23
C. Motivation to Combine Lim and Lillibridge	26
D. Guthrie	27
E. Motivation to Combine Lim and Guthrie.....	30
VIII. THE CHALLENGED '427 PATENT CLAIMS ARE UNPATENTABLE OVER THE PRIOR ART	31
A. GROUND 1: Claims 1, 5-6, 10-11, 15-16, and 20 Are Obvious Over Lim	31
1. Independent Claim 1	31
2. Claim 5.....	39
3. Claim 6.....	42
4. Claim 10.....	43
5. Independent Claim 11	48
6. Claim 15.....	50
7. Claim 16.....	50
8. Claim 20.....	50
B. GROUND 2: Claims 2-4 and 12-14 Are Obvious Over Lim Alone, As Well As Lim in Combination with Lillibridge	51
1. Claim 2.....	51
2. Claims 3-4.....	57

3.	Claim 12	59
4.	Claims 13-14	60
C.	GROUND 3: Claims 7-9 and 17-19 Are Obvious Over Lim Alone, As Well As Lim in Combination with Guthrie	60
1.	Claim 7	60
2.	Claim 8	66
3.	Claim 9	74
4.	Claim 17	78
5.	Claim 18	79
6.	Claim 19	79
IX.	SECONDARY CONSIDERATIONS	79
X.	CONCLUSION	80

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	10
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	7
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	20
<i>Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	10
<i>Tokai Corp. v. Easton Enters., Inc.</i> , 632 F.3d 1358 (Fed. Cir. 2011)	79
<i>Toyota Motor Corp. v. Cellport Sys., Inc.</i> , IPR2015-00633, Paper 11 (PTAB Aug. 14, 2015)	20
Statutes	
35 U.S.C. § 103	9
35 U.S.C. §§ 311-319	1
35 U.S.C. § 314	10-11
35 U.S.C. § 325	11
Rules and Regulations	
37 C.F.R. § 42	1, 4-9
Office Patent Trial Practice Guide, 77 Fed. Reg. 48759	4

LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 9,148,427 (the “’427 patent”)
1002	Prosecution History of U.S. Patent No. 9,148,427
1003	Declaration of Dr. Daniel Lopresti
1004	U.S. Patent No. 8,527,337 (“Lim”)
1005	Lim Provisional Application No. 60/144,612
1006	Lim Provisional Application No. 60/151,512
1007	Lim Provisional Application No. 60/201,539
1008	U.S. Patent No. 6,195,698 (“Lillibridge”)
1009	U.S. Patent No. 6,161,185 (“Guthrie”)
1010	U.S. Patent No. 7,197,639 to Juels
1011	European Patent EP1027639B1 to Suzuki
1012	Excerpts from Department of Defense, “Password Management Guideline”
1013	Excerpts from MITRE Corp. and U.S. Air Force, “Guidelines for Designing User Interface Software”
1014	U.S. Patent No. 5,826,015 to Schmidt
1015	“HTML Image Maps”
1016	“HTML ismap Attribute”
1017	“IMG extension for Mosaic 1.1”
1018	Excerpts from “HTML 3.2 Reference Specification”

Inter Partes Review

United States Patent No. 9,148,427

Exhibit	Description
1010	Excerpts from O'Reilly, "HTML The Definitive Guide"
1020	"Analysis of a Denial of Service Attack on TCP"

CHALLENGED CLAIM LISTING

Claim	Limitation No.	Limitation
1	[1-PRE]	A method for preventing robots from browsing a Web site beyond a welcome page, comprising:
	[1-A]	receiving an initial request, directed to the Web site, from an undefined originator; responding to the initial request with a challenge that prompts a response to the challenge from the undefined originator; and
	[1-B]	receiving the response to the challenge from the undefined originator, wherein the challenge includes: a plurality of graphical forms, and an accompanying textual expression describing one of the plurality of graphical forms, and the response to the challenge includes an identification of a location of the described one of the plurality of graphical forms.
2	2	The method of claim 1, further comprising modifying the challenge in response to a second initial request.
3	3	The method of claim 2, wherein the modifying includes varying a coordinate location of the described one of the plurality of graphical forms.
4	4	The method of claim 2, wherein the modifying includes varying which one of the plurality of graphical forms is described by the accompanying textual expression.
5	5	The method of claim 1, further comprising processing further requests from the undefined originator after the challenge has been successfully fulfilled.

Claim	Limitation No.	Limitation
6	6	The method of claim 1, further comprising stopping processing of further requests from the undefined originator after the challenge has not been successfully fulfilled.
7	7	The method of claim 6, wherein the stopping processing includes dropping or redirecting a TCP connection established with the undefined originator.
8	8	The method of claim 1, further comprising logging a source IP address of the undefined originator, and starting a timer.
9	9	The method of claim 1, further comprising: receiving a new request; determining whether a source IP address of the new request matches the logged source IP address of the undefined originator; determining whether said timer is expired; and upon the source IP address of the new request matching the logged source IP address of the undefined originator and the timer being expired, responding to the new request with a second challenge that prompts a response to the second challenge.
10	10	The method of claim 1, wherein the location is X and Y coordinates of the undefined originator's click associated with the challenge.
11	[11-PRE]	A computer program product comprising a non-transitory computer usable storage medium having stored therein computer usable program code for preventing robots from browsing a Web site beyond a welcome page, the computer usable program code, which when executed by a computer hardware device, causes the computer hardware device to perform:

Claim	Limitation No.	Limitation
	[11-A]	receiving an initial request, directed to the Web site, from an undefined originator; responding to the initial request with a challenge that prompts a response to the challenge from the undefined originator; and
	[11-B]	receiving the response to the challenge from the undefined originator, wherein the challenge includes: a plurality of graphical forms, and an accompanying textual expression describing one of the plurality of graphical forms, and the response to the challenge includes an identification of a location of the described one of the plurality of graphical forms.
12	12	The computer program product of claim 11, wherein the computer hardware device is further caused to perform modifying the challenge in response to a second initial request.
13	13	The computer program product of claim 12, wherein the modifying includes varying a coordinate location of the described one of the plurality of graphical forms.
14	14	The computer program product of claim 12, wherein the modifying includes varying which one of the plurality of graphical forms is described by the accompanying textual expression.
15	15	The computer program product of claim 11, wherein the computer hardware device is further caused to perform processing further requests from the undefined originator after the challenge has been successfully fulfilled.

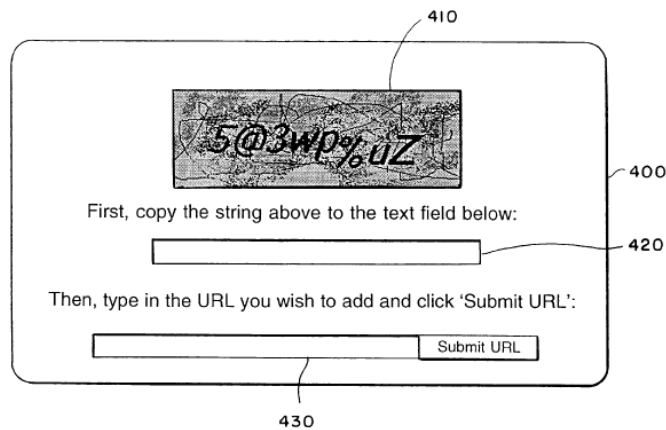
Claim	Limitation No.	Limitation
16	16	The computer program product of claim 11, wherein the computer hardware device is further caused to perform stopping processing of further requests from the undefined originator after the challenge has not been successfully fulfilled.
17	17	The computer program product of claim 16, wherein the stopping processing includes dropping or redirecting a TCP connection established with the undefined originator.
18	18	The computer program product of claim 11, wherein the computer hardware device is further caused to perform logging a source IP address of the undefined originator, and starting a timer.
19	19	The computer program product of claim 11, wherein the computer hardware device is further caused to perform: receiving a new request; determining whether a source IP address of the new request matches the logged source IP address of the undefined originator; determining whether said timer is expired; and upon the source IP address of the new request matching the logged source IP address of the undefined originator and the timer being expired, responding to the new request with a second challenge that prompts a response to the second challenge.
20	20	The computer program product of claim 11, wherein the location is X and Y coordinates of the undefined originator's click associated with the challenge.

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42, Petitioner respectfully requests *inter partes* review (“IPR”) of Claims 1-20 (“Challenged Claims”) of U.S. Patent No. 9,148,427 (the “’427 patent”).

The ’427 patent describes authentication methods to determine whether a user is human or a software agent (*i.e.*, a robot or “bot”) to stop bots from browsing websites. The system presents users with a challenge a human can answer but a bot is assumed to fail. Ex. 1001, Abstract.

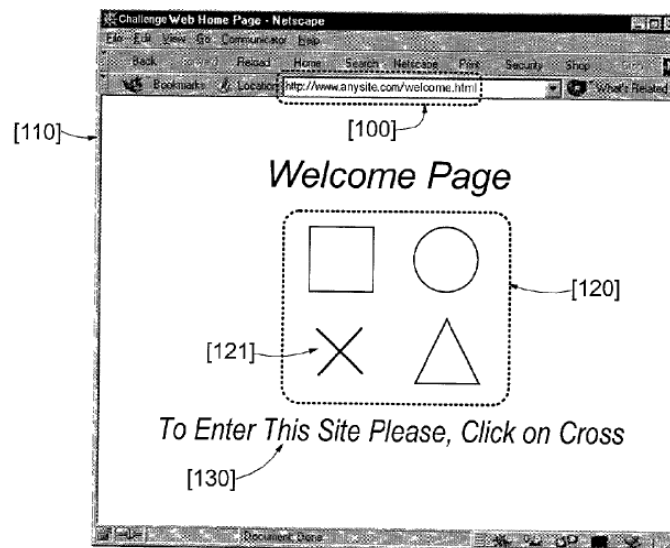
The patent admits distinguishing humans from bots, and the problems created by bots, were known issues for websites. Ex. 1001, 1:23-53, 2:8-12. The ’427 patent discloses posing Turing Tests to users to distinguish humans and bots. While not acknowledged in the patent, many Turing Tests to exclude bots from websites were in use prior to the invention of the ’427 patent, and this solution type was later named CAPTCHA. For example, the Lillibridge reference applied during prosecution discloses one of the first widely used CAPTCHAs, an image of distorted text that a user must read and enter into a prompt. Ex. 1008, Fig. 4:



Lillibridge also provides extensive background on existing prior art bot detection systems, issues regarding implementation of bot detection, and motivations for improvements to bot detection systems.

Faced with Lillibridge during prosecution, Patent Owner amended the claims to require a specific test embodied, for example, in the image below. Ex.

1001, Fig. 1:



Specifically, limitations were added requiring “a plurality of graphical forms[] and an accompanying textual expression describing one of the plurality of graphical forms,” prompting the user to identify the particular graphic described by the text. *See* Ex. 1002, 97-106. This was the only alleged point of novelty over Lillibridge.

However, this form of graphical challenge predates the '427 patent. For example, Lim taught exactly this sort of challenge. *See, e.g.,* Ex. 1004, Fig. 17 (colors added):

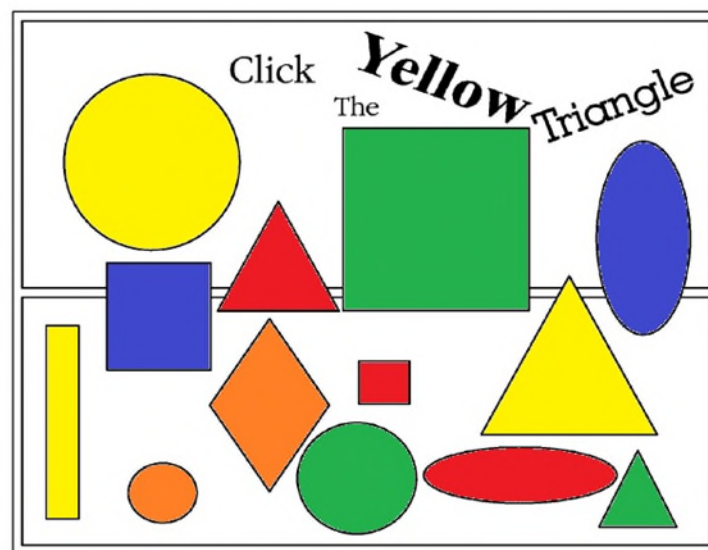


FIG. 17

Petitioner requests that the PTAB institute trial and find the Challenged Claims unpatentable for the reasons set forth herein.

II. 37 C.F.R. § 42.8(B): MANDATORY NOTICES

A. 37 C.F.R. § 42.8(b)(1): Notice of Real Parties-in-Interest

DataDome S.A. and DataDome Solutions, Inc. (“DataDome” or “Petitioner”) are the real parties-in-interest. No other parties exercised or could have exercised control over this Petition; no other parties funded or directed this Petition. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48759-60.

B. 37 C.F.R. § 42.8(b)(2): Notice of Related Matters

To the best knowledge of Petitioner, the ’427 patent has been involved in the following matters:

Case Name	Filed
<i>Arkose Labs Holdings, Inc. v. DataDome</i> , No. 1:23-cv-01467-RGA (D. Del.)	December 27, 2023

C. 37 C.F.R. § 42.8(b)(3) and (4): Notice of Counsel and Service Information

Petitioner's Lead Counsel	Petitioner's Back-Up Counsel
Richard F. Martinelli Reg. No. 52,003 Orrick, Herrington & Sutcliffe LLP 51 West 52nd Street New York, NY 10019-6142 RFMPTABDocket@orrick.com	Joseph A. Chern Reg. No. 63,246 Orrick, Herrington & Sutcliffe LLP 2050 Main Street, Suite 1100 Irvine, CA 92614-8255 2JAPTABDocket@orrick.com Tyler S. Miller Reg. No. 68,881 Orrick, Herrington & Sutcliffe LLP 51 West 52nd Street New York, NY 10019-6142 PTABDocketT5X@orrick.com

Petitioner submits a Power of Attorney with this Petition. Please address all correspondence to lead counsel. Petitioner consents to service by email at the email addresses listed above.

D. Fee for Inter Partes Review

The USPTO is authorized to charge the filing fee and any other fees incurred by Petitioner to the deposit account of Orrick, Herrington, & Sutcliffe LLP: 15-0665.

III. REQUIREMENTS FOR IPR

This Petition complies with all requirements under 37 C.F.R. § 42.104 for IPR.

A. § 42.104(a): Grounds for Standing

The '427 patent is available for IPR. Petitioner is not barred or estopped from requesting IPR. This Petition is timely filed under 35 U.S.C. § 315(b).

B. § 42.104(b): Identification of Challenge

Under 37 C.F.R. §§ 42.104(b) and 42.22, Petitioner requests that the Board institute IPR on the Challenged Claims of the '427 patent and cancel those claims as unpatentable.

1. § 42.104(b)(1): Challenged Claims

Petitioner challenges Claims 1-20 of the '427 patent.

2. § 42.104(b)(2): The Prior Art and Statutory Grounds

The application for the '427 patent claims priority to foreign application EP 00480085, filed on September 12, 2000.

While Patent Owner has not shown its claims have support for the September 12, 2000 priority date, the references relied upon herein are prior art by that date as follows:

Patent/Publication	Filing/Priority Date	Prior Art	Ex.
U.S. Patent No. 8,527,337 ("Lim")	July 20, 1999 (priority) July 18, 2000 (filing)	102(e)	1004 (Provisional Applications, Ex. 1005-1007)

Inter Partes Review

United States Patent No. 9,148,427

Patent/Publication	Filing/Priority Date	Prior Art	Ex.
U.S. Patent No. 6,195,698 ("Lillibridge")	April 13, 1998 (filing)	102(e)	1008
U.S. Patent No. 6,161,185 ("Guthrie")	March 6, 1998 (filing)	102(e)	1009

Because Patent Owner has not shown its claims have support prior to Lim's July 18, 2000 filing date, Petitioner does not need to establish that Lim is entitled to claim priority to any of its three listed provisional applications. *See* Ex. 1004, (60). However, if Patent Owner argues Lim is not prior art, all three of Lim's provisional applications provide full support under *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1379-80 (Fed. Cir. 2015).

While not required now, Petitioner provides limitation-by-limitation support in all three provisional applications for Lim Claim 1 and all concepts taught by Lim that are relied on in this Petition. Ex. 1003, Appendices B-D are charts comparing the applicable disclosures in Lim with corresponding disclosures in each of Lim's provisionals. *See* Ex. 1003, ¶¶69-72, Appendices B-D.

Lim's first provisional, application No. 60/144,612, was filed on July 20, 1999. Ex. 1005; Ex. 1004, (60). It fully supports Claim 1 of Lim and discloses all the concepts disclosed in Lim relied on in this Petition. Ex. 1003, ¶¶69-72, Appendix B.

Lim's second provisional, application No. 60/151,512, further elaborates on general, well-known principles of the Internet's operation and advertisement monetization, and was filed on August 30, 1999. Ex. 1006; Ex. 1004, (60). It fully supports Claim 1 of Lim and discloses all the concepts disclosed in Lim relied on in this Petition. Ex. 1003, ¶¶69-72, Appendix C.

Lim's third provisional, application No. 60/201,539, further elaborates on general, well-known principles of the Internet's operation, advertisement monetization, and example quizzes, and was filed on April 27, 2000. Ex. 1007; Ex. 1004, (60). It fully supports Claim 1 of Lim and discloses all the concepts disclosed in Lim relied on in this Petition. Ex. 1003, ¶¶69-72, Appendix D.

The non-provisional version of Lim again further elaborates on general, well-known principles of the Internet's operation and advertisement monetization, as compared to this third and final provisional. *Id.*, ¶¶69-72.

As shown in Ex. 1003, ¶¶69-72, Appendices B-D, each provisional fully supports Lim's disclosures and claims (*e.g.*, each of Lim's provisionals support both Claim 1 of Lim and the concepts disclosed in Lim relied on in this Petition). *Id.* Thus, in the event Lim must be shown to have a priority date earlier than its July 18, 2000 filing date, Lim is entitled to an effective filing date of July 20, 1999.

Below are the specific statutory grounds on which the claims are challenged:

Ground Number	Ground
1	Claims 1, 5-6, 10-11, 15-16, and 20 are obvious under 35 U.S.C. § 103 (pre-AIA) (“obvious”) over Lim alone
2	Claims 2-4 and 12-14 are obvious over Lim alone, as well as Lim in combination with Lillibridge
3	Claims 7-9 and 17-19 are obvious over Lim alone, as well as Lim in combination with Guthrie

Apart from Lillibridge, none of the references on which these grounds are based were before the Examiner during prosecution of the ’427 patent.

3. Level of Ordinary Skill in the Art

A POSITA in the technology described in the ’427 patent in 2000 would have had at least a Bachelor’s degree in computer science or computer engineering, or a similar discipline, along with 2-3 years of computer security, information security, or cybersecurity experience. Ex. 1003, ¶23. Relevant experience can substitute for education and vice versa. *Id.*

4. § 42.104(b)(5): Evidence Supporting Challenge

The Declaration of Dr. Daniel Lopresti (Ex. 1003) and other supporting evidence in the Exhibit List are filed herewith. Dr. Lopresti’s background and qualifications, and the information provided to him, are discussed in Exhibit 1003.

IV. INSTITUTION SHOULD BE GRANTED

This Petition establishes a reasonable likelihood of success on the merits and all other requirements for an IPR.

A. There Are No Grounds for a § 314 Discretionary Denial

There is a co-pending district court action involving the '427 patent. The Board considers the factors set forth in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) ("*Fintiv*") when determining institution in light of the pendency of such actions. As a whole, the *Fintiv* factors weigh strongly in favor of institution.

The district court litigation is at a very early stage and there has been little investment in the litigation by the court or parties. The case is currently awaiting decision on a motion to dismiss. DataDome has not answered the complaint, and no discovery or claim construction has occurred. This weighs in favor of institution. *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 8-9, 11 (PTAB June 16, 2020). No trial date has been set, so there can be no trial before the Board's projected statutory deadline. The court has not stayed the litigation. Other circumstances also weigh against the Board's exercise of discretion: there have been no other challenges to this patent and, as explained below, the Challenged Claims of the '427 patent are plainly unpatentable in view of the prior art.

Should Patent Owner urge the Board to exercise its discretion to deny institution, Petitioner respectfully requests a reply brief.

B. Denial Under § 325(d) Would Be Inappropriate

No ground presented here was considered by the Examiner or otherwise previously considered by the Patent Office. The primary reference, Lim, was not cited by the applicant or considered by the Examiner, and neither was Guthrie. Ex. 1001.

For these reasons, and as further explained below, the Board should institute IPR.

V. TECHNOLOGY BACKGROUND

By September 2000, the field of cybersecurity was well established and built upon the decades-old understanding of basic security principles. Ex. 1003, ¶27. The concept of using a challenge to distinguish genuine humans from automated agents or bots using Turing Tests was already well in place. *Id.* This included what is now commonly known as CAPTCHA, which stands for “Completely Automated Public Turing Test to tell Computers and Humans Apart,” a type of challenge-response authentication that distinguishes humans from bots. *Id.*

Tellingly, the ’427 Patent does not mention well-known prior art methods to distinguish humans from bots, which existed years before 2000. Ex. 1003, ¶28. For example, Lillibridge’s 1998 patent filing depicts precisely what we think of as

a CAPTCHA challenge—a string of random, distorted characters rendered into an image that is easy for a human to recognize but challenging for a bot. *Id.*; Ex.

1008, Fig. 4:

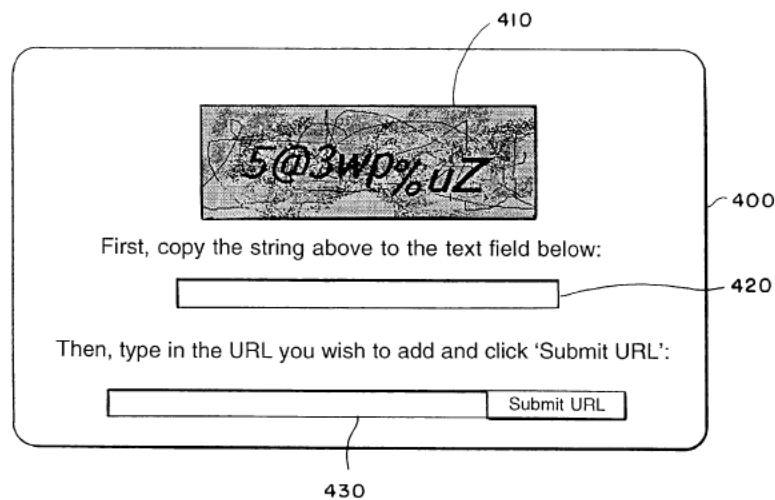


FIG. 4

Prior to 2000, the distorted text CAPTCHA shown in Lillibridge was in widespread use. Ex. 1003, ¶29. And POSITAs would have been familiar with CAPTCHAs, which merely apply the concept of the Turing Test (which dates back to 1950) to website access. *Id.* Turing Tests are a concept created by Alan Turing to determine whether software agents could pass for a human, which would signify artificial intelligence. *Id.* CAPTCHAs use software agents' inability to pass Turing Tests to conversely distinguish humans from bots, by exploiting the capability of humans to perform certain tasks better than a computer. *Id.* And Lim and Lillibridge demonstrate that detailed execution details and CAPTCHA test

variations were known years before the filing of the '427 Patent. *Id.*, ¶30.

Thus, by September 2000, the '427 patent was part of a crowded art where the concepts employed in the field were well understood, predictable, and routinely mixed and matched as needed to achieve a POSITA's design goals. Ex. 1003, ¶31. The particularities of such challenges—such as the exact form of the challenge, deploying challenges using standard TCP/IP communication protocols on the Internet, and the consequences of failing a challenge—were all known and available for designers to choose from to best accommodate their system, as discussed throughout this Petition. *Id.* For example, the well-known backgrounds of the TCP/IP communication protocol and lockout timers are discussed in Sections VIII.C.1 and VIII.C.2, respectively.

VI. THERE EXISTS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

The '427 patent aims to prevent robots from browsing websites by issuing a challenge to “undefined originators” making an initial request to access a site. Ex. 1001, Abstract. If the challenge is successfully fulfilled, the accessor is “assumed” to be a human; otherwise, the accessor is assumed to be a robot, and access is denied. *Id.* This is the basic, prior art, CAPTCHA concept. Ex. 1003, ¶34.

As the '427 patent explains, it was well known that servicing requests from bots could cause various problems, including using up valuable server time and

bandwidth, “swamp[ing] servers with rapid fire requests” in a Denial of Service (“DoS”) attack, traversing parts of servers not suitable for being searched, and slowing down the system. *Id.*, 1:23-50. Just as these problems were known, so were solutions that could “limit what the robot is allowed to do.” *Id.*, 1:51-53. The ’427 patent discusses prior art solutions that “rely on cooperation from the robots” (*e.g.*, the robots.txt protocol), which it considers inadequate for that reason. *Id.*, 1:53-2:7.

The ’427 patent also describes what it characterizes as the “standard way...to protect a Web site through some form of authentication,” which is by having registered users sign on with passwords. *Id.*, 2:8-16. The patent criticizes this method because it requires registration and management of the users. *Id.*, 2:12-25.

Critically, the ’427 patent did not identify other well-known methods for solving this problem at the time, such as CAPTCHA. Ex. 1003, ¶37.

By September 2000, online security was a crowded art, based on concepts that were well understood, predictable, and routinely combined as needed to achieve a POSITA’s design goals. *Id.*, ¶38.

A. Problem Addressed by the ’427 Patent and the Alleged Invention

The ’427 patent assumed existing systems for protecting websites required registration and management of a list of authorized users. Ex. 1001, 2:8-16.

With that framing, the patent identifies the object of the invention as “encourag[ing] human beings, attempting to access a robot protected Web site, to proceed further by not imposing a registration at first access and a log on procedure at each subsequent access.” *Id.*, 2:31-34. Instead, upon “receiving an initial request from an undefined originator, the Web site responds to the request with a welcome page including a challenge.” *Id.*, 2:46-50. The system assumes the user is human if the challenge is passed and a robot if it is failed. *Id.*, 2:50-57.

The '427 patent claims describe the specific format of this challenge, an example of which is shown in Figure 1:

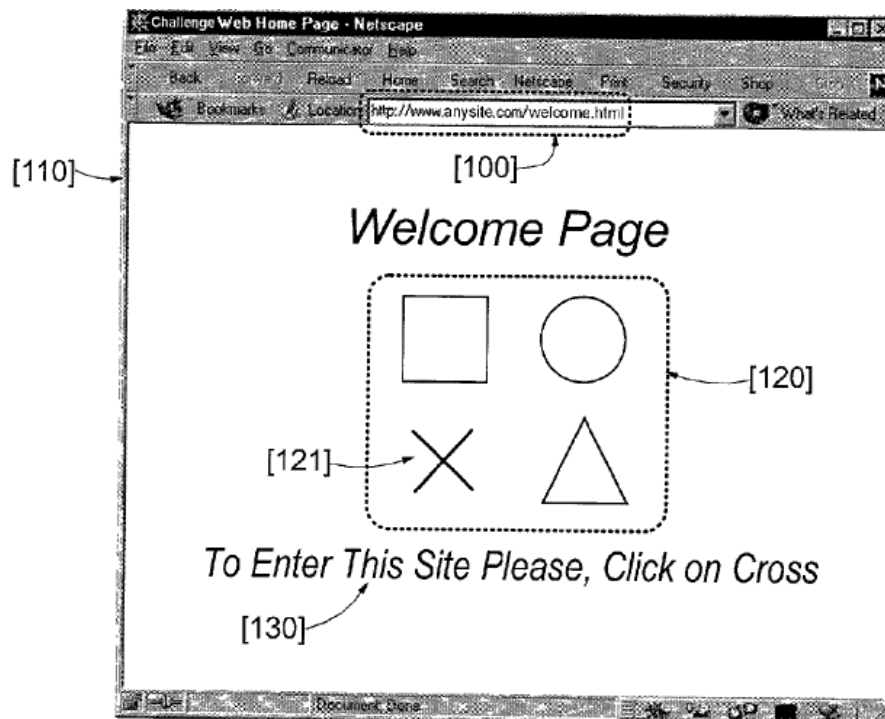


Figure 1

Ex. 1001, Fig. 1.

A user accessing a website is presented with the depicted challenge to test if the user is human. *Id.*, 3:10-24. The challenge includes “a few geometric forms” 120—here a square, circle, cross and triangle. *Id.*, 3:24-31. These images “can be unambiguously referred to by a single word or expression in a language that the individual accessing the Web is assumed to be capable of reading.” *Id.* The text 130 prompts the user to select one of the images, here by clicking on cross 121. *Id.*

The '427 patent states a human will “naturally” follow the instruction and click on the cross, while a robot “will do nothing, or will do it wrongly simply because it just does not understand the graphic symbols or which of them may be a cross.” *Id.*, 3:31-35. “Hence, this invention easily allows discrimination of a human being from a robot on the basis of their respective levels of abstract reasoning, which is naturally high, or very high, for a human being while a robot is totally lacking this capacity.” *Id.*, 3:35-39.

The patent’s other challenge embodiments, Figures 5-a and 5-b, demonstrate variations of the graphical challenge. Ex. 1001, Figs. 5-a, 5-b:

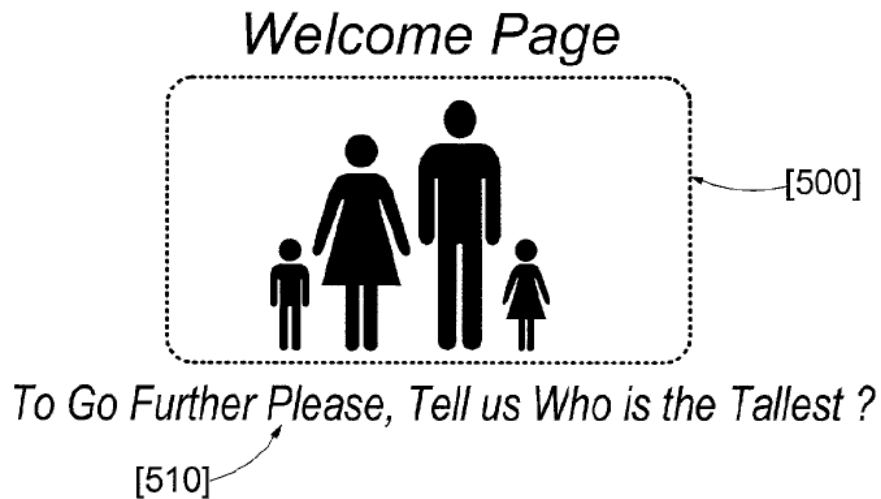


Figure 5-a

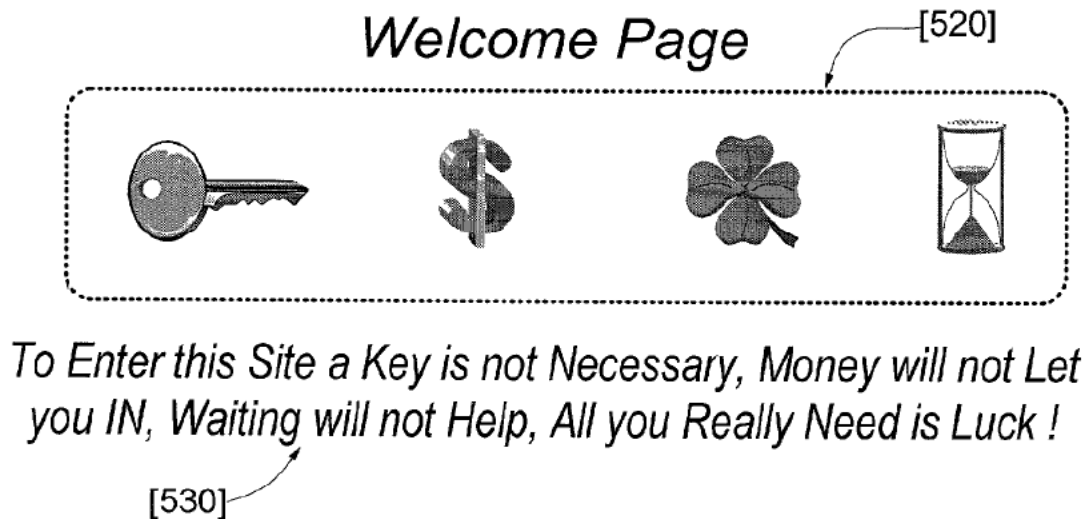


Figure 5-b

See also 4:44-57.

B. Prosecution History

The '427 patent stems from foreign application EP 00480085 and was prosecuted in the United States as Application No. 12/113,607.

On August 27, 2010, the PTO rejected all pending claims over Lillibridge. *See* Ex. 1002, 68-77. The patent owner entirely rewrote the claims and argued the prior art of record did not teach that “the challenge includes: a plurality of graphical forms, and an accompanying textual expression describing one of the plurality of graphical forms, and the response to the challenge includes an identification of a location of the described one of the plurality of graphical forms.” *See* Ex. 1002, 97-106.

On February 17, 2011, another Office Action issued rejecting the new claims. *See* Ex. 1002, 110-121. The applicant responded that “[i]ntegral to [the independent claims] is that the challenge includes a plurality of graphical forms and an accompanying textual expression describing one of the plurality of graphical forms.” *Id.*, 146-167 (July 13, 2011 Appeal Brief) at p. 7; *see also id.* at pp. 7-8 (applicant arguing that “in the Appellants’ claimed invention the accompanying textual expression provides the answer to the challenge (not just instruction to select or enter a personal password)”).

In response to additional rejections (*see id.*, 173-184), the applicant further characterized the purported invention on appeal, distinguishing the applied *Blonder* reference as follows:

Blonder teaches a graphical password arrangement that displays a predetermined graphical image and requires a user to “touch” predetermined areas of the image in a predetermined sequence, as a

means of entering a password. ... First, it is noted that in Blonder there is only one graphical image, not a plurality of graphical forms. Second, in Blonder the user is prompted to touch predetermined areas of the image in a predetermined sequence. Therefore, in Blonder the prompt instructs what the user is required to do, but does not describe one of the plurality of graphical forms.

Id., 194-215 (March 15, 2012 Appeal Brief) at p. 10.

The PTAB accepted the applicant's arguments, stating:

...the Examiner relies on a disclosure in Blonder to provid[e] a prompt along with the password image as part of the challenge provided to the user. The prompt is interpreted by the Examiner to be the textual expression accompanying one of the plurality of graphical forms as it describes an action to be taken on a particular icon/tap region. However, the claim language requires the textual expression describe one of the plurality of graphical forms. The section of Blonder relied upon by the Examiner relates to the setting of a password by tapping various regions on a graphical image. A prompt instructs a user to select a tap region and position it within the password region. We do not find this prompt to describe one of the plurality of graphical forms as required by the claims.

Id., 235-244 (March 3, 2015 Decision on Appeal) at pp. 7-8 (citations omitted).

The pending claims were allowed without further substantive responses. *See id.*, 245-252 (May 18, 2014 Notice of Allowance).

In sum, throughout prosecution, the applicant consistently argued its invention is a challenge that includes both a **plurality** of graphics or images and an accompanying textual expression that instructs the user to select **one** of those graphics. Ex. 1003, ¶53. As shown by the prior art discussed in this Petition, that concept was far from inventive at the time. *Id.*

C. Claim Construction

The Board construes claims under *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*) and its progeny. Under *Phillips*, claims are given their plain and ordinary meaning in light of the specification. 415 F.3d at 1315-17. The Board only construes claim terms when necessary to resolve the controversy. *See, e.g., Toyota Motor Corp. v. Cellport Sys., Inc.*, IPR2015-00633, Paper 11 at 16 (PTAB Aug. 14, 2015). Petitioner does not believe any claim construction is necessary here.

VII. THE PRIOR ART

A. Lillibridge

Lillibridge explains that Internet service providers “may want to restrict their servers to only human users” because automated agents, *i.e.*, bots, can mimic human user access and are known to be “malicious, destructive, or otherwise annoying.” Ex. 1008, 1:20-28. Lillibridge further identifies several specific scenarios where allowing agents could be harmful: polls, advertising, spam email, search engine manipulation, access to proprietary information (*e.g.*, web scraping). *Id.*, 1:29-2:14. Lillibridge explains that in the above Internet scenarios “it is difficult for the server computers to differentiate requests submitted by users from those generated by an agent.” *Id.*, 2:15-18. Lillibridge criticizes prior approaches as working “only for specific contexts of a particular service” and not applicable to

“any type of Web server.” *Id.*, 2:41-46. Lillibridge further describes an October 1996 Digital Equipment Corp. polling Website that tried to secure its polling data by having a user click on an image of a flag to gain access to the poll (“the DEC System”) and criticizes it because it would be easy for a computer to do. *Id.*, 2:47-59. In particular, the DEC System polling website gave the same test to every user and only required clicking on one image, as opposed to selecting among images.

With this background, Lillibridge identified “a need for a server computer to be able to distinguish an ordinary user from an automated agent so that access to the agent can be denied, and while permitting access to real human users.” Ex. 1008, 2:60-64. Lillibridge proposes a server that receives a request from an unknown client and issues a “riddle” in the form of a string of human-perceptible characters that are randomly selected and modified (*e.g.*, by distorting the characters or overlaying them on a “noisy” background). *Id.*, 3:6-20. This allows the creation of different quizzes for different users, addressing the deficiencies of the DEC System, which provided a single quiz problem to all users. Ex. 1003, ¶57.

Lillibridge’s Fig. 3 shows the creation of an example riddle, and Fig. 4 shows the presentation of that riddle to the client. Ex. 1008, Figs. 3-4:

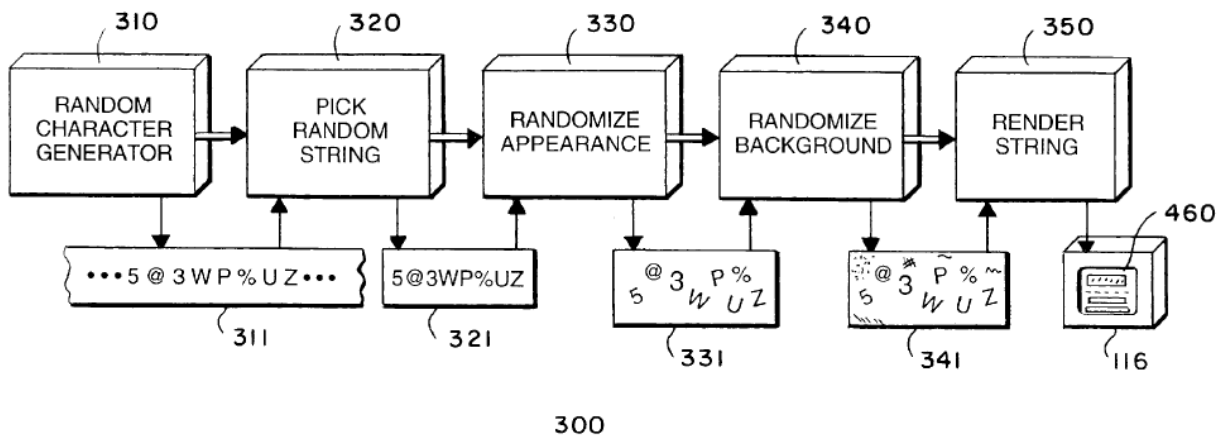


FIG. 3

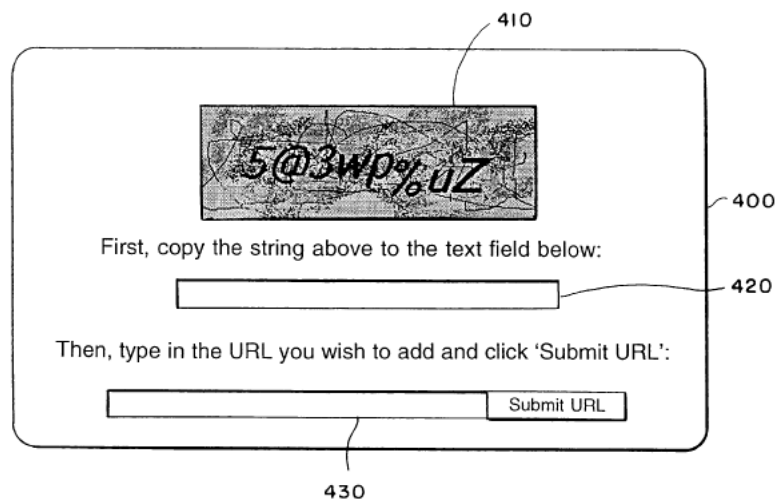


FIG. 4

The server distinguishes between a human client and an “automated agent,” based on whether the correct answer is timely provided. Ex. 1008, 3:21-34; Ex. 1003, ¶¶55-59. This is the basic CAPTCHA concept. Ex. 1003, ¶59.

Lillibridge represents a common early example of what we now call a CAPTCHA. Ex. 1003, ¶60. Its April 1998 disclosure shows the conceptual

solution of using riddles or quizzes to distinguish humans from bots was already known years before the '427 patent. *Id.*, ¶61; Ex. 1008, (22).

As discussed above in Section VI.B, the '427 patent's prosecution history shows the only claimed concept that Lillibridge does not allegedly teach is the particular type of puzzle claimed—one that has a **plurality** of graphics or images with an accompanying textual expression instructing the user to select **one** of those graphics. Ex. 1003, ¶61. However, Lim disclosed a number of embodiments of this same challenge before the '427 patent. *Id.*

B. Lim

Like Lillibridge, Lim teaches using quizzes to stop bots from accessing websites, but Lim's challenges include graphically-based, multiple-choice pictures and prompts like the '427 patent. Ex. 1004, Abstract. Assigned to Google, Lim shows some of the many ways that Google was already using what would later be coined CAPTCHA technologies to provide online security in 1999 and 2000. Ex. 1004, (73); Ex.1003, ¶62.

Lim described various challenges that combine a plurality of graphics and textual expressions instructing users to select one graphic. As Lim explains, its challenges can verify “whether or not an Internet operation (*e.g.*, sending an e-mail message or accessing a web site) is being attempted by a human being or an automated process...by using a quiz process that requires user interaction.” Ex.

1004, 2:32-38. “Quizzes may be used as part of a process to verify that a user is human, as opposed to an automated process (e.g., a bot or robot).” *Id.*, 13:15-18.

Lim’s quizzes rely on pictures or other images because bots will not be able to decipher the question or the answer from the image, while humans can do so easily. Lim further explains the importance of quizzes that are simple for humans because the goal is not to test the human’s knowledge. Ex. 1004, 13:40-49; Ex. 1003, ¶¶63-64.

For implementation, Lim explains text box inputs could be used or, for multiple-choice questions, “the answers might be selectable from the image itself, *e.g.*, using an image map.” Ex. 1004, 13:52-56. Lim inspires POSITAs to vary its example quizzes, “any of which may be used in combination with one another or individually.” *Id.*, 13:57-59. For example, one quiz spells out the name of a recognizable object, such as “a dog, book, a car, [or] the word ‘Ice Cream,’” and users are asked to select the correct picture or word matching the object. *Id.*, 13:63-14:5. A variety of quiz examples are provided using this structure, such as shape identification, color recognition, and questions containing the answer. *Id.*, 14:7-23.

Lim describes numerous quizzes that are answered by clicking on an identified object. For example, “simple counting” challenges are also discussed, in which a “number of similar object[s] are displayed, such as 2 balls, 4 birds, 1

finger, etc.,” and users may be “asked to select the picture, word or number matching the object displayed” and/or “asked to select the set of pictures showing the same number of objects.” Ex. 1004, 14:24-30; *see also* 14:31-41 (“simple computations,” such as the question “2 cats+2 dogs” instructing the user to select the picture showing “2 cats+2 dogs”), 14:42-48 (“simple queries,” where users respond to simple questions by “‘clicking’...on the right area”).

These concepts are further depicted in Fig. 17, which asks a user to “[c]lick on the yellow triangle.” Ex. 1004, 14:51-53; *id.*, Fig. 17 (colors added):

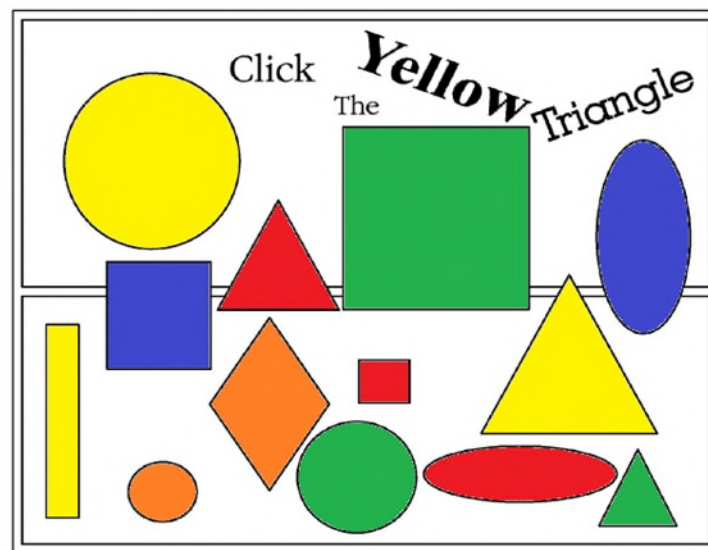


FIG. 17

Lim thus not only provides numerous examples of the same challenges the '427 patent Challenged Claims recite—challenges including a plurality of graphics and an accompanying textual expression instructing the user to select one of

them—but also employs them in the same context as the '427 patent—determining whether someone accessing a website is human or a robot. Ex. 1003, ¶¶65-68.

C. Motivation to Combine Lim and Lillibridge

A POSITA would have found it obvious to combine Lim and Lillibridge for many reasons. Ex. 1003, ¶¶73-77.

Lim and Lillibridge are in the same field, Internet authentication and security, are directed to the same specific problem—distinguishing humans and bots in evaluating unknown users of websites—and address that problem by providing tests that would be easy for humans but difficult for bots. *See, e.g.*, Ex. 1004 (Lim), Abstract, 2:32-38, 13:15-18, 13:40-49; Ex. 1008 (Lillibridge), 1:20-28, 2:15-18, 2:60-64; Ex. 1003, ¶74.

Lim and Lillibridge even expressly address this problem for the same use cases, such as preventing advertising fraud. *See, e.g.*, Ex. 1004 (Lim), 13:40-51; Ex. 1008 (Lillibridge), 1:40-46; Ex. 1003, ¶75.

Further, both references are implemented on the World Wide Web using standard network technologies. *See, e.g.*, Ex. 1004 (Lim), 1:35-2:9, 4:7-24, 5:6-7:61, 8:18-56, 23:3-43, Figs. 1, 16; Ex. 1008 (Lillibridge), 1:13-19, 2:66-3:5, 3:55-4:6, Fig. 1; Ex. 1003, ¶76. A POSITA could have predictably and successfully combined them without undue experimentation. *Id.*

Additional details regarding why a POSITA would have been motivated to

combine Lim and Lillibridge to arrive at the particular claims at issue are discussed in Section VIII.B.1 below. For example, a POSITA would have recognized the benefit of varying Lim's quizzes from one request to the next based on Lillibridge's express disclosure of generating a modified riddle for each request, to enhance Lim's security. Ex. 1003, ¶77.

D. Guthrie

Guthrie teaches the secure authentication of a client to a server over a network such as the Internet. Ex. 1009, 1:12-19, 3:53-5:15, Figs. 1A-1B:

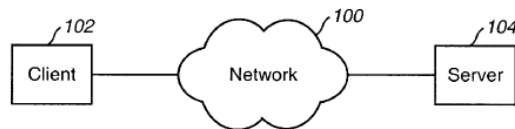


FIG. 1A

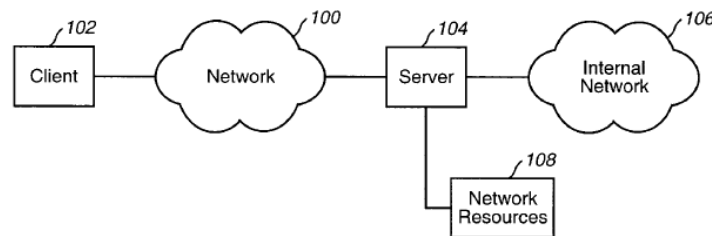


FIG. 1B

Guthrie explains “user authentication, rather than simply machine or system authentication,” is improved by distinguishing legitimate human users from “a system that has been pre-programmed with access information (e.g., running a ‘script’ to permit access).” Ex. 1009, 1:29-37. Guthrie recognizes that bots’

ability to rapidly make many attempts to defeat an authentication must be protected against. Ex. 1003, ¶79.

Guthrie teaches that, when a client's user fails the authorization process, a "lock-out timer" is set by the server. Ex. 1009, 8:10-12. "The purpose of the lock-out timer is to thwart an unauthorized user from repeatedly 'hammering' the server 104 manually **or through an automated application** with authorization attempts, while still eventually allowing a legitimate user access to the server 104." *Id.*, 8:24-30 (emphasis added). Guthrie explains that the lockout timer is set to prevent the user from accessing the server only for a certain amount of time, which prevents rapid-fire authentication attempts. *Id.*, 8:18-23; Ex. 1003, ¶80.

During authorization, the server checks a data structure like user account table 200 to see if the lock-out timer flag 212 has been set for this user. Ex. 1009, 7:64-8:10, Fig. 6:

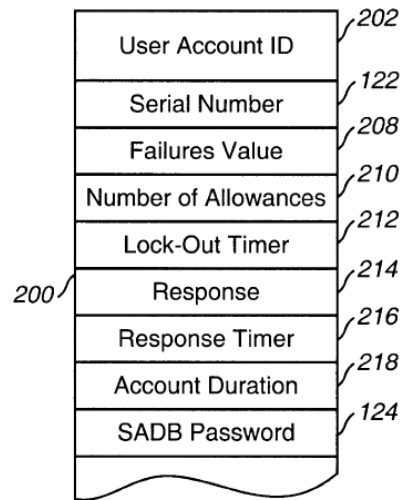


FIG. 6

If the flag is set and the lockout timer has not expired, access is denied. Ex. 1009, 9:6-10. If the flag is not set or the timer has expired, authorization continues. *Id.*, 8:7-10, 9:6-10, Fig. 7A:

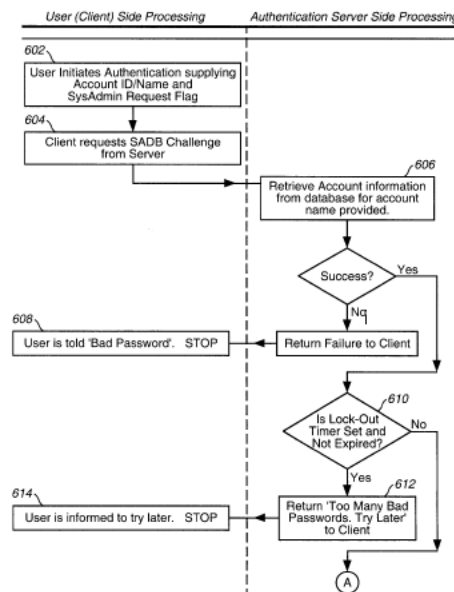


FIG. 7A

See also Ex. 1009, 11:42-59, 12:6-9, Figs. 8A-8B.

Guthrie explains how lockout timers can be used in Internet security procedures to prevent “automated” applications (*e.g.*, bots) from accessing a server, while still allowing legitimate human users to access the server after the lockout timer expires, without banning them forever due to a simple error. Ex. 1009, 8:24-30; Ex. 1003, ¶¶78-84.

E. Motivation to Combine Lim and Guthrie

A POSITA would have found it obvious to combine Lim and Guthrie for many reasons. Ex. 1003, ¶¶85-88.

Lim and Guthrie are in the same field, Internet authentication and security, disclose lockout timers, and are directed to the same specific problem—distinguishing humans and bots in evaluating unknown website users. *See, e.g.*, Ex. 1004 (Lim), Abstract, 2:32-38, 13:15-18, 13:40-49; Ex. 1009 (Guthrie), 1:12-19, 1:29-37, 3:53-5:15, Figs. 1A-1B; Ex. 1003, ¶86.

The references are implemented on the World Wide Web using standard network technologies. *See, e.g.*, Ex. 1004 (Lim), 1:35-2:9, 4:7-24, 5:6-7:61, 8:18-56, 23:3-43; Ex. 1009 (Guthrie), 1:12-19, 4:50-5:15, Figs. 1A-1B; Ex. 1003, ¶87. Thus, a POSITA could have predictably and successfully combined them without undue experimentation.

Additional details regarding why a POSITA would have been motivated to combine Lim and Guthrie to arrive at the claims at issue are discussed in Section

VIII.C.2 below. For example, a POSITA would have been inspired to combine Guthrie's lockout timer with Lim's quizzes, to accomplish Lim's user suspension for a set time after a failed authorization attempt, without blocking human users permanently. Ex. 1003, ¶88.

VIII. THE CHALLENGED '427 PATENT CLAIMS ARE UNPATENTABLE OVER THE PRIOR ART

A. GROUND 1: Claims 1, 5-6, 10-11, 15-16, and 20 Are Obvious Over Lim

1. Independent Claim 1

Lim renders Claim 1 obvious. Ex. 1003, ¶¶91-119.

a) [1-PRE]

To the extent the preamble is found to be limiting, Lim discloses and renders obvious “[a] method for preventing robots from browsing a Web site beyond a welcome page.” Ex. 1003, ¶¶92-95.

Lim discloses “a process for verifying whether or not an Internet operation (*e.g.*, sending an e-mail message or ***accessing a web site***) is being attempted by a human being or an automated process [that] may be implemented by using a quiz process that requires user interaction.” Ex. 1004, 2:33-39 (emphasis added); *see also, e.g.*, Abstract, 13:15-28 (quizzes “may be used as part of a process to verify that a user is a human”), 8:25-30, Claim 1, Fig. 1.

Lim explains that when a user reaches a website's welcome page, “new

users may be asked to answer one or more questions of a quiz to test whether they are a human user[] or not,” so that robots are excluded. Ex. 1004, 9:45-67.

Thus, Lim’s quiz challenges comprise methods for preventing robots from browsing a website beyond a welcome page. Ex. 1003, ¶¶92-95.

b) Element [1-A]

Lim discloses and renders obvious “receiving an initial request, directed to the Web site, from an undefined originator” and “responding to the initial request with a challenge that prompts a response to the challenge from the undefined originator.” Ex. 1003, ¶¶96-99.

Lim’s quiz challenges are issued in response to an initial request from an unknown user (*i.e.*, an undefined originator) to access a website. Ex. 1003, ¶97. Lim’s challenges are applied to new users accessing a website to verify whether access “is being attempted by a human being or an automated process” and “may be implemented by using a quiz process that requires user interaction.” Ex. 1004, 2:33-39; *see also, e.g.*, Abstract, 9:46-67 (new users are “referred to a service provider’s Web site” and “may be asked to answer one or more questions of a quiz to test whether they are a human users or not”), 13:15-28, Claim 1 (claiming “granting the human operator access to a computer-based resource” when they are determined to be human by fulfilling a challenge sent in response to an initial request from an unknown user); Ex. 1003, ¶¶97-98. Because these are **new** users,

they are an undefined originator making an initial request. Ex. 1003, ¶98.

Lim thus receives and responds to an undefined originator's initial request with a challenge that prompts a response from the originator. Ex. 1003, ¶¶96-99.

c) Element [1-B]

Lim discloses and renders obvious “receiving the response to the challenge from the undefined originator, wherein the challenge includes: a plurality of graphical forms, and an accompanying textual expression describing one of the plurality of graphical forms, and the response to the challenge includes an identification of a location of the described one of the plurality of graphical forms.” Ex. 1003, ¶¶100-119.

Lim's quiz challenges are posed to new, unknown users (*i.e.*, undefined originators). See Section VIII.A.1.b; Ex. 1003, ¶101; Ex. 1004, Abstract, 2:33-39, 9:53-67, 13:15-28, Claim 1.

Lim discloses many quiz challenges, any of which can be implemented using multiple graphics or images (*i.e.*, a plurality of graphical forms) and text that describes one of those graphics (*i.e.*, an accompanying textual expression describing one of the plurality of graphical forms). Ex. 1003, ¶¶102-119.

Lim's system uses challenges, which display a number of graphical objects and provide a text prompt to select one object, to distinguish humans from robots. Ex. 1004, Claim 1 (“transmitting...a prompt including one or more graphical

images, and a means for a human operator of the second computer system to provide a respective response thereto, the prompt presented in a format sufficient to permit the human operator of the second computer system, but not an automated process executing thereon, to read the prompt and provide a corresponding single correct and distinct response to the respective prompt presented by said graphical image”), 2:37-39, 13:29-37; Ex. 1003, ¶103.

The prompts for any of Lim’s quiz questions may be presented as “text that is embedded in graphical representations such as an image,” *i.e.*, as graphical text. Ex. 1004, 13:29-37; Ex. 1003, ¶104; *see also* Ex 1004, 13:64-65 (prompt presented “in graphical text”), 14:42-43 (“[u]sers are asked simple questions using graphical text”). While not required by the claim, Lim provides extra security compared to plain text by presenting the quiz questions “using a display format that cannot be easily recognized or read by a machine or automated process.” *Id.*; Ex. 1003, ¶105; Ex. 1004, 14:8-11.

Lim further expressly discloses that its quiz questions can be “multiple-choice questions,” in which case the user is prompted to click the described answer graphic “from the image itself, *e.g.*, using an image map, and/or through an HTML form surrounding the picture.” Ex. 1004, 13:54-56; Ex. 1003, ¶106.

Because Lim’s multiple-choice questions are image-based, a POSITA would understand two things about them. Ex. 1003, ¶¶107-108. First, as an image-based

multiple-choice question, the question would include a plurality of graphical forms for the user to pick from. Ex. 1003, ¶107; Ex. 1004, 13:67-14:5 (users are asked “to select the correct picture...matching the object displayed” or “to identify the one object that does not belong in a set of objects being displayed”), 14:24-25 (a “number of similar object[s] are displayed”), 14:38-39, 14:51-53, Fig. 17.

Second, because Lim’s graphical text prompt directs the user to select one of the graphical forms and the user responds by clicking the described answer graphic “from the image itself, *e.g.*, using an image map,” the user would respond by clicking on the location of the described graphic (*i.e.*, an identification of a location of the described one of the plurality of graphical forms). Ex. 1003, ¶108; Ex 1004, 13:54-56, 14:34-39, 14:43-45 (responses “selected by ‘clicking’ (*e.g.*, using a cursor control device such as a mouse) on the right area”), 14:51-53 (“Click on a Designated Object/Space...*e.g.*, ‘Click on the yellow triangle’”), Fig. 17. Lim’s graphical text prompt thus describes one of the graphics, and the user responds by clicking on its location. Ex. 1003, ¶108. An image map is a standard HTML input method to accomplish this by providing a server with the location of a user’s click in x,y coordinates and a POSITA would understand Lim’s image map to operate this way. *Id.*

A POSITA would have further understood that Lim teaches that any of its example quiz prompts can be implemented in this format—a multiple-choice

question responded to using an image map. Ex. 1003, ¶109. This is particularly so due to Lim's express statement that any of its "various types of quizzes" "may be used in combination with one another," explaining that any of their attributes can be readily combined. *Id.*; Ex. 1004, 13:57-59.

The example quiz of Fig. 17 shows graphics depicting several shapes in different colors, and a textual expression describing one and instructing the user to select it: "[c]lick on the yellow triangle." Ex. 1003, ¶110; Ex. 1004, 14:51-53 ("Click on a Designated Object/Space. Users are asked to select a particular image, e.g., 'Click on the yellow triangle.'"), Fig. 17 (colors added):

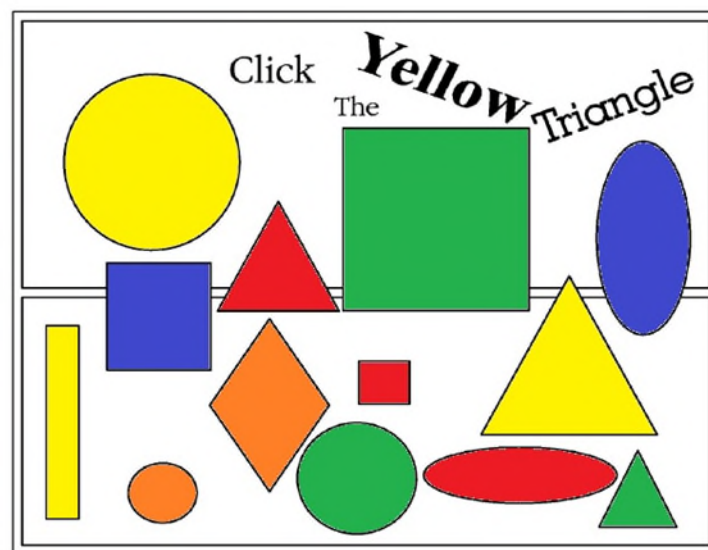


FIG. 17

The picture contains a plurality of graphical forms (*i.e.*, the colored shapes), and the graphical text query (*i.e.*, "click the yellow triangle") is an accompanying textual expression describing one of the plurality of graphical forms (*i.e.*, the

yellow triangle). Ex. 1003, ¶111.

Lim discloses additional examples of this concept in its “simple word/object identification/recognition” challenges, which can include a prompt wherein a “word is spelled out in graphical text” and ask users to “select the correct picture.” Ex. 1004, 13:63-14:5. Lim teaches that such a challenge can be implemented using multiple-choice questions, an image map showing a plurality of graphical forms, and questions presented in graphical text. *Id.*, 13:54-56. Following Lim’s teaching would result in a question presented in graphical text describing an object (*e.g.*, click on the hat) and multiple objects displayed (*e.g.*, pictures of a hat, shovel, and frying pan). Ex. 1003, ¶112. Thus, this challenge directly aligns with ’427 patent Fig. 1. *Id.*; Ex. 1001, Fig. 1:

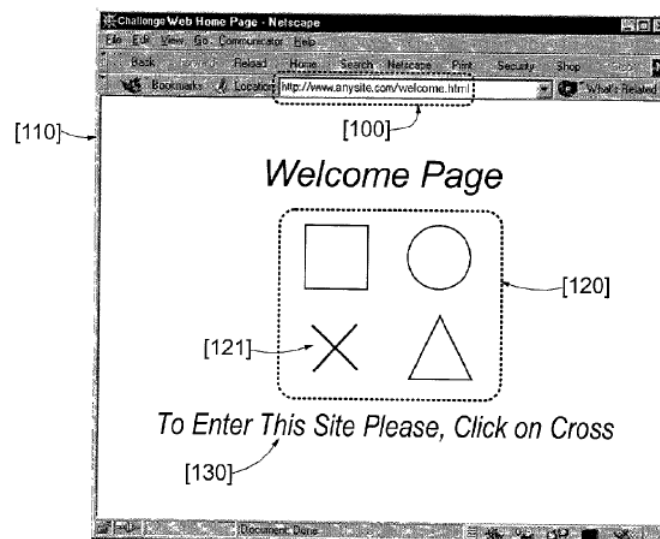


Figure 1

These simple challenges can also ask users to “identify the one object that

does not belong in a set of objects being displayed.” Ex. 1004, 13:63-14:5. This challenge can also be implemented using multiple-choice questions and an image map as described above, which aligns with ’427 patent Fig. 5-b. Ex. 1003, ¶¶113-114; Ex. 1001, Fig. 5-b:

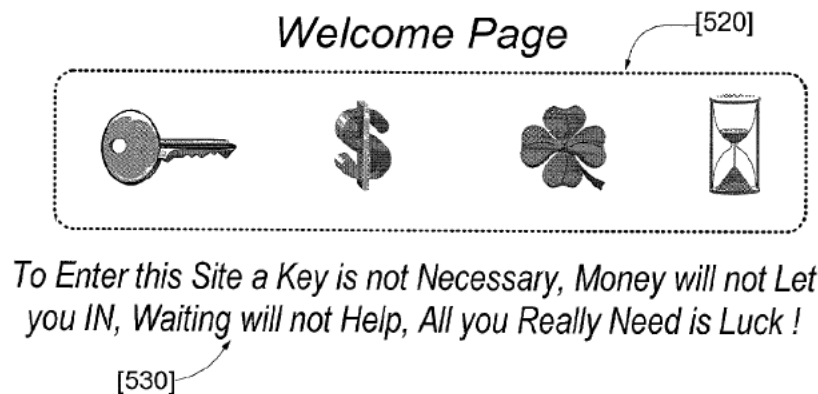


Figure 5-b

Lim’s many other types of quizzes can also be implemented using multiple-choice questions and an image map in this same way. Ex. 1003, ¶115.

For example, Lim’s “simple counting” challenges can be multiple-choice, displaying a plurality of graphics (*e.g.*, graphics showing 2 balls, 4 birds, and 1 finger) and an accompanying textual expression describing one of the graphics (*e.g.*, graphical text stating select the 2 balls), and can be responded to by having the user click on the correct location on the image map (*e.g.*, clicking on the 2 balls graphic). Ex. 1004, 14:24-30; Ex. 1003, ¶116.

Similarly, the “simple computations” challenges can be multiple-choice,

displaying a plurality of graphics (*e.g.*, graphics showing the numbers 1-3), and an accompanying textual expression describing one of the graphics (*e.g.*, text stating what is 1+1), and can be responded to by having the user click on the correct location on the image map (*e.g.*, clicking on the number 2 graphic). Ex. 1004, 14:31-41; Ex. 1003, ¶117.

Lim’s “simple queries” also can be multiple-choice, displaying a plurality of graphics (*e.g.*, graphics showing a flame and a snowflake), and an accompanying textual expression describing one of the graphics (*e.g.*, text stating “[i]s ice cream hot or cold?”), and can be responded to by having the user click on the correct location on the image map (*e.g.*, clicking on the snowflake graphic). Ex. 1004, 14:42-48; Ex. 1003, ¶118.

In sum, Lim not only provides numerous examples of the challenge the ’427 patent recites—multiple-choice challenges including a plurality of graphics and an accompanying textual expression instructing the user to select one of them, which the user responds to by clicking the instructed graphic on an image map—but also employs them in the same context as the ’427 patent—determining whether someone accessing a website is a human or a robot. Ex. 1003, ¶119.

2. Claim 5

Claim 5 depends from Claim 1 and further requires “processing further requests from the undefined originator after the challenge has been successfully

fulfilled.”

Lim discloses and renders obvious this additional limitation. Ex. 1003, ¶¶121-128.

As discussed above for Claim 1, Lim presents an unknown, new user (*i.e.*, undefined originator) with a challenge to determine whether they are a human or a robot. See Section VIII.A.1; Ex. 1003, ¶122.

If the undefined originator successfully responds to the challenge, the additional limitation of Claim 5 requires processing at least one or more requests from the undefined originator. Ex. 1003, ¶123. Lim discloses processing multiple requests and how to allow a POSITA to adjust the number of requests that are processed. *Id.*

Lim explains that, if the unknown user succeeds at the challenge, because they have been determined to be a human, their request to access the computer system will be granted and their further requests will also be processed. Ex. 1004, Claim 1 (“determining, by the first computer system, whether the respective response matches its corresponding single correct and distinct response: when so, inferring that the respective response was provided by the human operator of the second computer system and granting the human operator access to a computer-based resource” and “determining an amount of time or amount of resources that will be accessible by the human operator before a next prompt is transmitted”),

Abstract, 2:32-39, 8:19-30, 9:45-67, Fig. 1; Ex. 1003, ¶124.

Lim provides additional detail about how subsequent requests can be handled in its Fig. 5 embodiment. Ex. 1003, ¶125; Ex. 1004, Fig. 5:

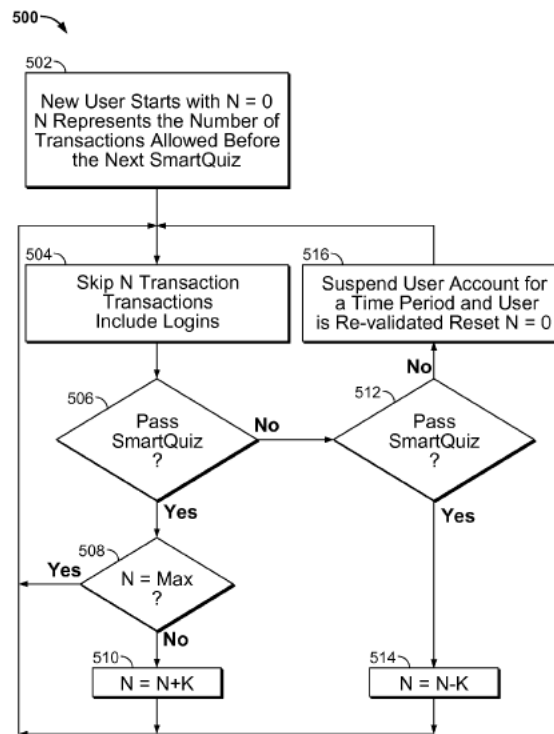


FIG. 5

As Lim explains, a new user is immediately presented with a first quiz. Ex. 1004, 14:58-15:2; Ex. 1003, ¶126. If they pass the first quiz (step 506), because the variable N , which represents the number of allowed transactions for the user before being quizzed, begins at 0 (step 508), it may be incremented, $N+K$ (step 510). *Id.* The user is then able to engage in K transactions without being quizzed again (step 504). *Id.* By selecting K (and thereby N), Lim provides the system designer with the flexibility to choose the number of transactions before a retest.

Ex. 1003, ¶127. In other words, the server processes a designer selected number of requests from the undefined originator after the challenge has been successfully fulfilled, which satisfies Claim 5. *Id.*, ¶128.

3. Claim 6

Claim 6 depends from Claim 1 and further requires “stopping processing of further requests from the undefined originator after the challenge has not been successfully fulfilled.”

Lim discloses and renders obvious this additional limitation. Ex. 1003, ¶¶130-132.

As discussed for Claim 5, Lim explains that the users’ further requests are processed if they succeed at the challenge. Ex. 1003, ¶131. Likewise, if the user fails the quiz, access will be blocked. *Id.*, ¶132; Ex. 1004, Claim 1, 9:59-67 (“quizzes may be introduced at various levels to thwart such automated processes and allow access only by live, human users”), 14:67-15:2 (on failure, “suspend[] the user’s account for a designated time interval or cause[] some other penalty”), Fig. 5:

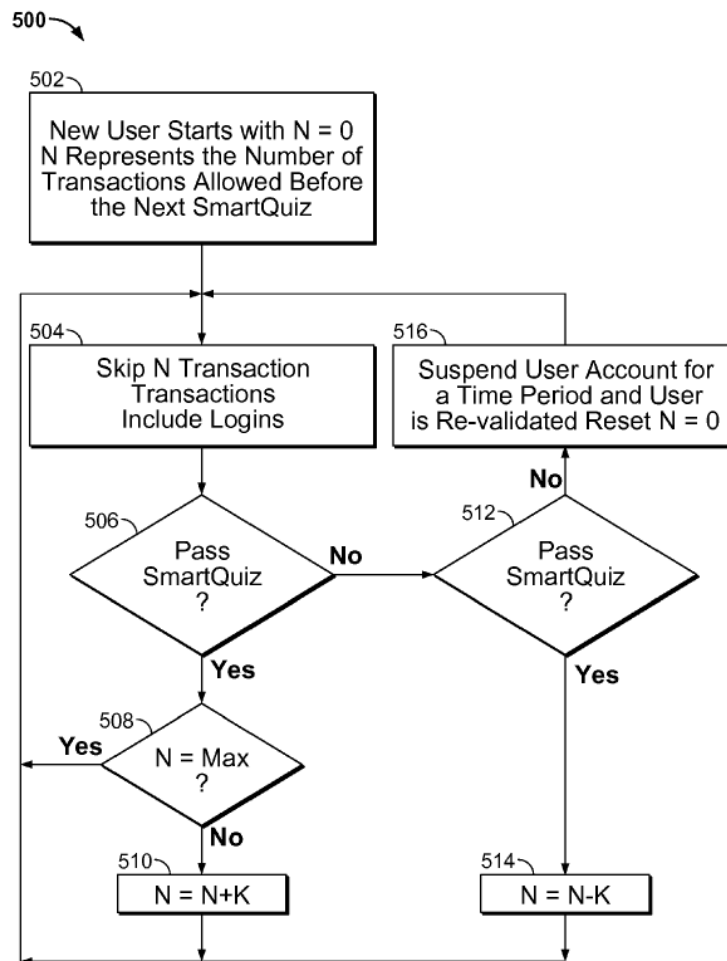


FIG. 5

See also Abstract, 2:32-39, 9:45-59, 14:58-67, Fig. 1.

4. Claim 10

Claim 10 depends from Claim 1 and further requires that “the location is X and Y coordinates of the undefined originator’s click associated with the challenge.”

Lim discloses and renders obvious this additional limitation. Ex. 1003, ¶¶134-151.

HTML image maps were a well-known, simple way of creating distinct clickable areas on an image, implemented by setting a list of coordinates for a specific image that hyperlink ***different parts*** of the image to ***different web addresses***, without having to divide the image into separate files. Ex. 1003, ¶135.

As reflected by Lim's use of them, image maps have been part of the web since the 1990s and have not changed materially since then. *Id.*, ¶136. For example, as implemented from the beginning, image maps have long been used to set the coordinates for part of an image (*e.g.*, the computer below) to link to a separate webpage than other parts of the image. *Id.*, ¶¶136-141 (referencing

https://www.w3schools.com/html/html_images_imagemap.asp) (Ex. 1015):



Because image maps rely on X-Y coordinates, a POSITA would have understood that user selections made by clicking on an image map require obtaining the X-Y coordinates of the user's click, or at a minimum that it would have been obvious to do so. Ex. 1003, ¶142.

Lim expressly explains that users may respond to its quiz challenges by clicking on the location of the correct image with a cursor control device such as a mouse, using an image map. Ex. 1004, 13:54-56 (“For multiple-choice questions, the answers might be selectable from the image itself, *e.g.*, using an image map”), 14:42-48 (“Responses may be...selected by ‘clicking’ (*e.g.*, using a cursor control device such as a mouse) on the right area.”), 14:51-53 (“Users are asked to select a particular image, *e.g.*, ‘Click on the yellow triangle.’ (See *e.g.*, FIG. 17.)”), Fig. 17. A visual example showing the location of the yellow triangle as the correct location to be clicked is shown in Fig. 17, using an image map. Ex. 1003, ¶144; Ex. 1004, Fig. 17 (colors added):



Of the two ways to implement an image map, server-side or client-side, it would have been most obvious for a POSITA to implement Lim's image map on the server side, both because it would have been obvious to try the two limited alternatives, and also because there are distinct security advantages to a server-side image map in the context of Lim's multiple-choice guesses. Ex. 1003, ¶146. Bots

could read the HTML code of client-side image maps, greatly reducing the number of possible answers. *Id.* A POSITA would have readily found it much simpler, straightforward, and secure to implement Lim's image maps on the server-side to accomplish Lim's goal of effectively distinguishing between humans and bots. *Id.*

Lim's server-side image map would have been implemented using the HTML-standard "ismap" attribute, which specifies that the image is part of a server-side image map, so that when the user clicks on the image, the coordinates of their clicks are sent to the server as a URL query string. Ex. 1003, ¶147; *see also* https://www.w3schools.com/TAGs/att_ismap.asp (Ex. 1016). The "ismap" attribute was widely in this way used prior to the '427 Patent. *Id.*, ¶148; *see also* <http://1997.webhistory.org/www.lists/www-talk.1993q2/0343.html> (Ex. 1017) (use in Mosaic web browser Version 1.1 in 1993); <http://www.comfsm.fm/computing/html3.2/index.html> (Ex. 1018) (discussion in HTML 3.2 Reference Specification, January 1997); <https://www.openeye-training.com/downloads/HTMLcomp.pdf> (Ex. 1019) (discussion in O'Reilly's "HTML The Definitive Guide," August 1998). Indeed, the '427 Patent's identification of how to implement this X-Y coordinate embodiment is using the "ismap" attribute. *Id.*, ¶149; Ex. 1001, 3:54-67, Fig. 2.

The obviousness of having Lim process user interactions with its image maps using the X-Y coordinates of the user's clicks is confirmed by examples of

using click coordinates in this way in additional prior art. Ex. 1003, ¶¶149-150; see European Patent EP1027639B1 to Suzuki (Ex. 1011), ¶¶0019-0022, 0036, Figs. 2 (steps S20-S24), 3C (showing calculation of coordinates of points selected by user and discussing processing user mouse clicks “by subtracting the coordinates of the image origin from the point’s coordinates,” including “the case of a point whose location is specified by (xs, ys).”).

It is thus obvious to a POSITA that Lim’s use of an image map in interpreting a user’s selection of a particular graphic within an image on a GUI through a mouse click would have been implemented by determining the X-Y coordinates of the location the user clicked. Ex. 1003, ¶151.

5. Independent Claim 11

Lim renders Claim 11 obvious. Ex. 1003, ¶¶152-157.

a) [11-PRE]

To the extent the preamble is found to be limiting, Lim discloses and renders obvious “[a] computer program product comprising a non-transitory computer usable storage medium having stored therein computer usable program code for preventing robots from browsing a Web site beyond a welcome page, the computer usable program code.” Ex. 1003, ¶¶153-156.

For example, Lim’s Fig. 1 discloses a basic system architecture embodiment comprising users 100a-c, who are attempting to access content sources 108a-108c

via network 102 (e.g., the Internet). Ex. 1004, 8:18-30, Fig. 1:

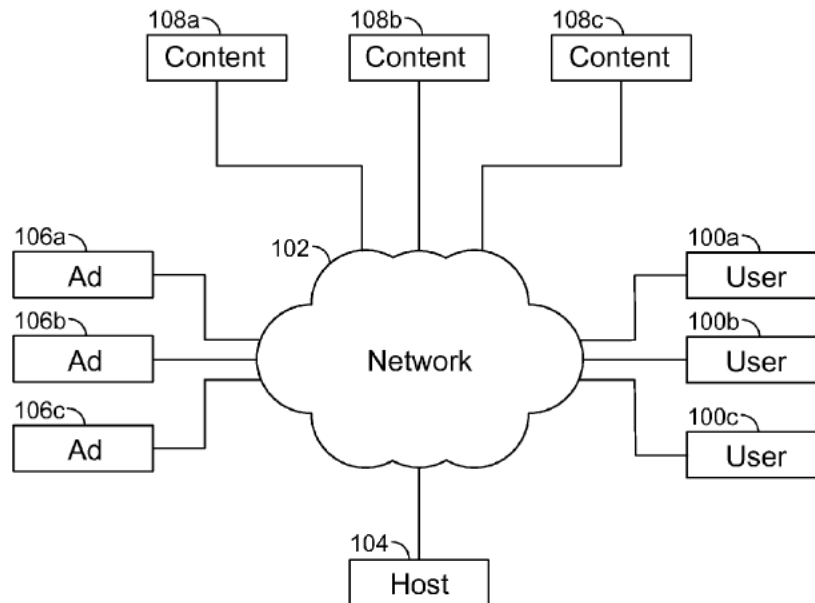


FIG. 1

Host 104 is “made up of one or more computers, a cluster of computers, a web or server farm, and/or some other configuration of one or more computers.” Ex. 1004, 8:52-56. The “embodiments of the invention (which may be computer software, hardware and/or combinations of both) are discussed as being hosted/provided by or from the host 104,” but there may be multiple hosts and content may be provided by other sources. *Id.*, 8:58-65. As computers, host(s) run computer program code stored on a computer usable non-transitory medium. Ex. 1003, ¶155.

The functionalities performed by the code stored on host 104 thus include

the functionalities for preventing robots from browsing a website beyond a welcome page discussed above for the preamble of Claim 1 and are disclosed by Lim for the reasons discussed above for that preamble. *See* Section VIII.A.1; Ex. 1003, ¶156.

b) Elements [11-A]-[11-B]

Elements [11-A]-[11-B] are the same as Elements [1-A]-[1-B]. Thus, Lim discloses and renders obvious these portions of Claim 11 for the same reasons discussed above for Claim 1. *See* Section VIII.A.1; Ex. 1003, ¶157.

6. Claim 15

Claim 15 depends from Claim 11. The additional limitation of Claim 15 is the same as that of Claim 5. Thus, Lim discloses and renders obvious Claim 15 for the same reasons discussed above for Claim 5. *See* Section VIII.A.2; Ex. 1003, ¶¶158-159.

7. Claim 16

Claim 16 depends from Claim 11. The additional limitation of Claim 16 is the same as that of Claim 6. Thus, Lim discloses and renders obvious Claim 16 for the same reasons discussed above for Claim 6. *See* Section VIII.A.3; Ex. 1003, ¶¶160-161.

8. Claim 20

Claim 20 depends from Claim 11. The additional limitation of Claim 20 is

the same as that of Claim 10. Thus, Lim discloses and renders obvious Claim 20 for the same reasons discussed above for Claim 10. See Section VIII.A.4; Ex. 1003, ¶¶162-163.

B. GROUND 2: Claims 2-4 and 12-14 Are Obvious Over Lim Alone, As Well As Lim in Combination with Lillibridge

As discussed above, Lim discloses and renders obvious Claims 1 and 11. See Section VIII.A; Ex. 1003, ¶164. The additional limitations of Claims 2-4 and 12-14 are obvious over Lim alone, as well as Lim in combination with Lillibridge. Ex. 1003, ¶165.

1. Claim 2

Claim 2 depends from Claim 1 and further requires “modifying the challenge in response to a second initial request.”

Lim renders this additional limitation obvious, both alone and in combination with Lillibridge. Ex. 1003, ¶¶167-185.

Of course, new users will get new quizzes because using the same quiz for all users would be easily thwarted. Ex. 1003, ¶¶171-172. Lim explains that a user is given subsequent quiz challenges in the form of a “second prompt” or “next prompt” (*i.e.*, a second initial request) after a set time interval has passed after the initial challenge (*i.e.*, the initial request). *Id.*, ¶¶168-169; Ex. 1004, 14:58-15:2 (a new user “is presented with a series of SmartQuizzes (step 506), with subsequent

quizzes presented at an interval determined based on their success or failure (step 504)'), Fig. 5:

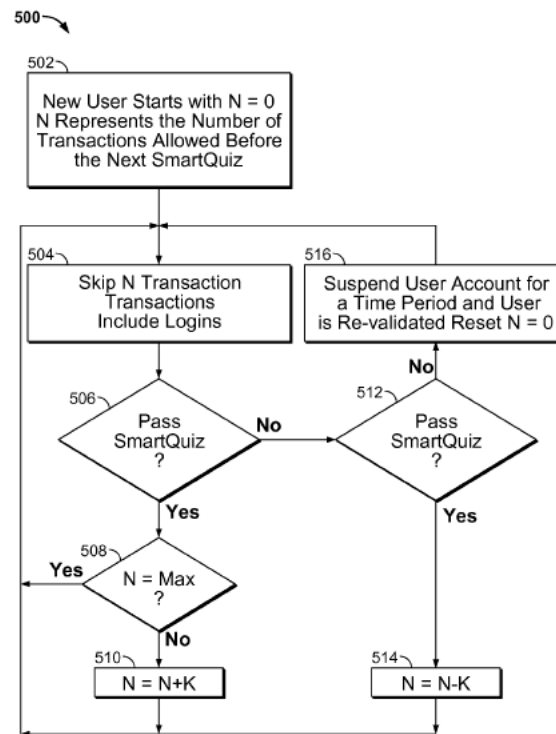


FIG. 5

Thus, a POSITA would have understood that Lim's second quiz challenges are sent when a user tries to access the same website or resource after the set interval has passed, such that their next (or continued) access would be considered a second initial request. Ex. 1003, ¶170; Ex. 1004, Claim 1, 14:58-15:2.

A POSITA also would have understood that these subsequent quiz challenges would not have included the same questions as the initial challenges (*i.e.*, they are modified versions of the initial challenge) because Lim rewards users for multiple correct answers by delaying the time between quizzes. Ex. 1003,

¶¶171-174.

A POSITA would have understood this in view of Lim's express disclosure that one application of its quizzes involves allowing advertisers to effectively present advertisements to human users. Ex. 1003, ¶172; Ex. 1004, 4:7-35, 7:62-8:17, 8:30-35, 9:20-30, Fig. 1. Indeed, Lim explains that one of the express purposes of its quizzes is to protect against advertising fraud, where bots generate false advertisement "views" rather than the actual human intended to view the advertisements. *Id.*; Ex. 1004, 13:40-51 ("Because automated entities are not able to decipher the question... advertisers are provided with some assurance that their advertising dollars are not being wasted"). This application of Lim would not work if all users were given the same challenge as their initial requests because bad actors would easily automate giving the correct answer to other bots. *Id.* Similarly, if the same user was given the same quiz every time, a human could correctly answer the question once and then give the answer to a bot, allowing the bot to simply repeat the answer every time and drive up false advertising revenue. *Id.*

This concern is reflected in Lim's Fig. 5. Ex. 1003, ¶173. Specifically, when a user succeeds at a quiz (step 506), "N," the number of transactions they can engage in before having to take another quiz (step 504), can be increased up to a maximum amount (steps 508, 510). Ex. 1004, 14:58-65, Fig. 5:

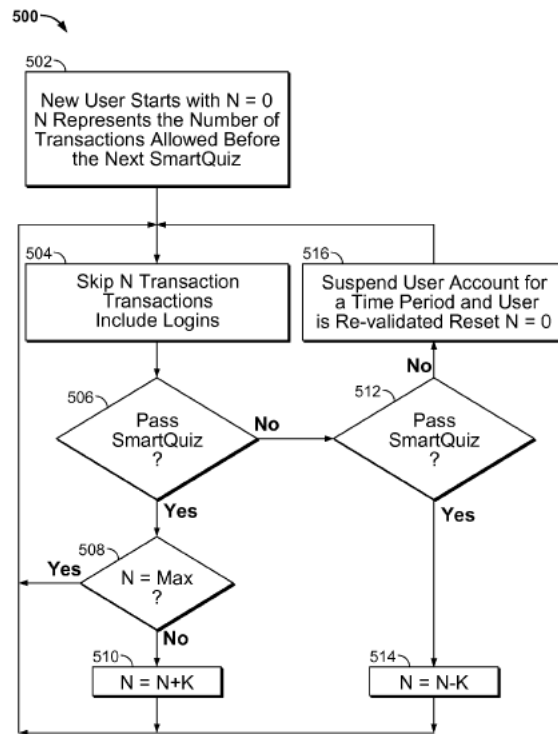


FIG. 5

Lim's use of the N variable, as incremented by an additional K transactions up to a maximum amount, allows the site provider to flexibly set the cadence to balance user annoyance at having to answer a quiz against the risk the user has turned the system over to a bot and increase that cadence as a reward for multiple correct answers. Ex. 1003, ¶174. Lim's reward-based increases to K call for different quizzes because there is no reason to increasingly reward the user for passing the same test. *Id.* Moreover, each quiz after N transactions would need to be different to avoid the trivial process of automating bot answers to the same repeated question. *Id.*; see also Ex. 1008, 2:47-59 ("it is easy to write a program that recognizes the American flag...in a random position on the screen...and

simulates a click; therefore, this method does not effectively restrict access by electronic agents”). Lim’s focus on advertising, where serving ads to bots could have significant negative financial consequences, motivates avoiding repeated quizzes that are easily defeated. *Id.*

This understanding is confirmed by Lim’s statements that its subsequent quizzes are a distinct “next prompt” or “second prompt” and that each of its many challenge embodiments may be used in combination with one another or individually, suggesting a readiness to revise and modify its challenges. Ex. 1003, ¶175; Ex. 1004, Claim 1 (“next prompt” or “second prompt”), 3:23-26 (“various types of quizzes, any of which may be used in combination with one another or individually”), 3:64-67, 13:57-59, 14:58-15:2, Figs. 5, 17.

Even putting the above aside, a POSITA would have found it obvious to modify the quiz of Lim in view of Lillibridge. Ex. 1003, ¶176.

A POSITA would have been motivated to combine Lim and Lillibridge for at least the reasons discussed in Section VII.C above and as follows. *Id.*, ¶177.

Lim provides an extensive list of example quiz types that can be used. Ex. 1003, ¶178. This provides a POSITA implementing its system many, varied quizzes and quiz types and supports the obvious notion that many quizzes would be needed. *Id.*

Lillibridge provides a complementary teaching emphasizing the use of

modifiable quizzes to satisfy many applications. Ex. 1003, ¶179. Lillibridge explains that its quizzes can be used to fairly conduct lotteries, popularity contests, or polls (Ex. 1008, 1:29-39), limit email spam (*id.*, 1:47-57), prevent search engine “page boosting” (*id.*, 1:59-2:7), prevent bots from accessing proprietary information (*id.*, 2:8-13), and, like Lim, prevent advertising fraud (*id.*, 1:40-46), which demonstrates a need for multiple changing challenges. Ex. 1003, ¶179.

Like Lim’s, Lillibridge’s challenges are riddles that test if a user is a human or “electronic agent.” *See generally*, Ex. 1008, 3:55-6:16; Ex. 1003, ¶180.

Lillibridge explains that, by default, it “require[s] the user to solve one riddle for each request.” Ex. 1008, 8:48-49; *see also* 9:3-9 (discussing a riddle being sent out each time an email is sent). This describes the generation of a modified riddle for every request. Ex. 1003, ¶181. Lillibridge also notes that this default could be relaxed to “present a new riddle less frequently,” such as every five requests. *Id.*; Ex. 1008, 8:48-52, Claim 39.

A POSITA would thus understand each of Lillibridge’s embodiments to describe generating a random riddle with each request. Ex. 1003, ¶182.

In sum, a POSITA reading Lim would have would have been motivated and found it obvious that the same riddle should not be repeated in a row, to effectively protect against bots. Ex. 1003, ¶183. Lillibridge’s teaching further confirms the security benefits of generating a new or modified riddle for each request. *Id.*

A POSITA thus would have considered it obvious to apply these teachings in Lillibridge to Lim's quizzes and would have been motivated to combine Lillibridge's riddle modification teachings with Lim's quizzes in order for Lim to accomplish Lim's security goals more effectively. Ex. 1003, ¶184. Legitimate human users would easily adapt to modified riddles, while bots would not. *Id.* In contrast, bots would be able to take advantage of unchanging riddles, undermining Lim's security goals. *Id.*

A POSITA would have further been motivated to form this combination because both Lim and Lillibridge are attempting to achieve the same goal in the same context: effectively distinguishing humans from bots among unknown users attempting to access an Internet resource. Ex. 1003, ¶185; Ex. 1004, 9:46-67, 13:15-28; Ex. 1008, 1:20-28, 2:60-63, 4:30-38, 6:11-16, 9:36-40.

2. Claims 3-4

Claim 3 depends from Claim 2 and further requires that "the modifying includes varying a coordinate location of the described one of the plurality of graphical forms."

Claim 4 depends from Claim 2 and further requires that "the modifying includes varying which one of the plurality of graphical forms is described by the accompanying textual expression."

Lim renders these additional limitations obvious, both alone and in

combination with Lillibridge. Ex. 1003, ¶¶187-198.

As discussed above for Claim 2, Lim explains that a user is given subsequent quiz challenges in the form of a “second prompt” or “next prompt,” and sets forth a motivation to modify these subsequent quizzes to prevent advertising fraud. See Section VIII.B.1; Ex. 1003, ¶190; Ex. 1004, Claim 1, 13:40-51, 14:58-15:2, Fig. 5.

As also discussed above, Lillibridge expressly discloses generation a modified riddle for each request, providing further motivation for changing subsequent riddles to enhance security. See Section VIII.B.1; Ex. 1003, ¶191; Ex. 1008, 7:29-50, 7:64-8:5, 8:13-14, 8:20-26, 8:48-52, 9:3-9, Claim 39. Lillibridge thus motivates a POSITA to modify Lim’s quizzes to achieve Lillibridge’s enhanced security benefits. See Section VIII.B.1; Ex. 1003, ¶191.

A POSITA also would have understood that one obvious way to modify Lim’s quizzes would have been to change the location of the graphic identified by the text. Ex. 1003, ¶¶195-196. They also would have understood that another obvious way to modify Lim’s quizzes would have been to change which graphic is identified by the text. *Id.*, ¶¶197-198.

These are two of a few ways to simply modify Lim’s multiple-choice image map quizzes. Ex. 1003, ¶¶192-193. A POSITA would have had a strong motivation to make many different quizzes and versions of quizzes when

implementing a system like Lim's to avoid workarounds to the quizzes that would have been trivial for bots to use. *Id.* If the same quiz or a limited number of quizzes are commonly reused, bad actors would program a bot to specifically recognize that quiz. *Id.* Indeed, Lillibridge notes that the DEC quiz, where every user was asked the same question—"click on the flag"—with the same American flag, shown in a different location each time, was too trivial. *Id.*; Ex. 1008, 2:47-59.

There are only a few limited ways to make numerous versions of the multiple-choice picture quizzes taught by Lim: 1) changing the text prompt to ask the user to click a different object; 2) changing the location of the objects; 3) using different objects; or 4) a combination of the above. Ex. 1003, ¶193. Due to the need to provide many quizzes, a POSITA would be motivated to use all of these options. *Id.*, ¶194. But of these options, changing the location of the object identified by the text and changing the text to identify a different object are two of the easiest options because they reuse the object images, which are more costly to locate or create, compared to merely changing the text or object location. *Id.*

3. Claim 12

Claim 12 depends from Claim 11. The additional limitation of Claim 12 is the same as that of Claim 2. Thus, Claim 12 is obvious over Lim alone, and Lim in combination with Lillibridge, for the same reasons discussed above for Claim 2.

See Section VIII.B.1; Ex. 1003, ¶¶199-200

4. Claims 13-14

Claims 13 and 14 depend from Claim 12. The additional limitations of Claims 13 and 14 are the same as those of Claims 3 and 4. Thus, Claims 13 and 14 are obvious over Lim alone, and Lim in combination with Lillibridge, for the same reasons discussed above for Claims 3 and 4. See Section VIII.B.2; Ex. 1003, ¶¶201-202.

C. GROUND 3: Claims 7-9 and 17-19 Are Obvious Over Lim Alone, As Well As Lim in Combination with Guthrie

As discussed above, Lim discloses and renders obvious Claims 1 and 11, as well as Claims 6 and 16. See Section VIII.A; Ex. 1003, ¶203. The additional limitations of Claims 7-9 and 17-19 are obvious over Lim alone, as well as Lim in combination with Guthrie. Ex. 1003, ¶204.

1. Claim 7

Claim 7 depends from Claims 1 and 6 and further requires that “the stopping processing includes dropping or redirecting a TCP connection established with the undefined originator.”

Lim renders this additional limitation obvious, both alone and in combination with Guthrie. Ex. 1003, ¶¶206-228.

TCP/IP, often referred to as the “Internet protocol suite,” is a standard

framework for organizing the set of communication protocols for communicating on the Internet and other computer networks. Ex. 1003, ¶207. It was the dominant standard for Internet communications by at least the early 1990s, and as its name suggests, it involves the use of two complementary protocols—IP, or “Internet Protocol,” the network layer communications protocol for relaying information over a network, and TCP, or “Transmission Control Protocol,” the transport layer communications protocol for communicating with the application layer and transporting the data. *Id.*, ¶¶208-210.

A POSITA in 2000 would have been very familiar with TCP/IP and would have understood that reference to either of TCP or IP also means the use of the other. Ex. 1003, ¶211. Thus, they would have understood that network communications made using IP addresses would have been suspended or ended by dropping or redirecting a TCP connection. *Id.*

As discussed above for Claim 6, Lim discloses that: 1) its system is designed to protect web servers; 2) when an unknown user fails a challenge their account will be suspended; and 3) during the time when a user’s account is suspended, the processing of their requests is stopped because they have been determined to be a robot. See Section VIII.A.3; Ex. 1003, ¶212; Ex. 1004, Claim 1, 9:59-67, 14:67-15:2, Fig. 5.

Lim also explains that its network communications are conducted over the

Internet and involve communications made using IP addresses. Ex. 1003, ¶213;

Ex. 1004, Figs. 1, 16:

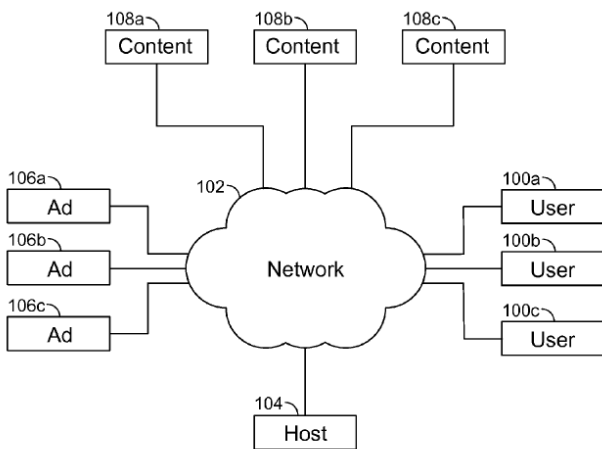


FIG. 1

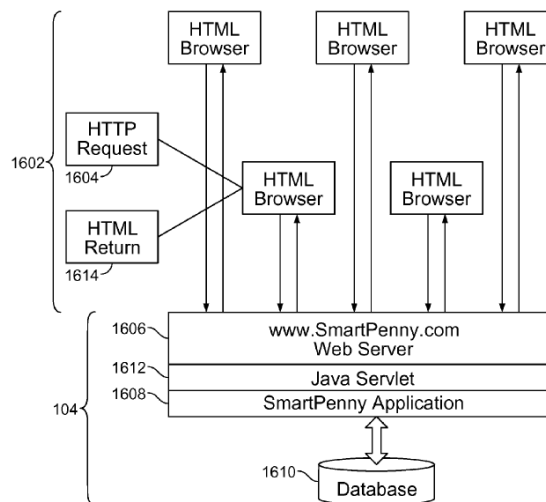


FIG. 16

See also Ex. 1004, 5:6-6:30 (discussing ordinary use of IP addresses to access websites), 8:19-56, 23:4-43 (discussing use of conventional HTTP requests). Lim expressly discusses limiting or restricting the number of users using unique identifiers such as the user's IP address. Ex. 1004, 13:4-14. Because the user's IP address identifies the client and is part of the TCP/IP protocol, this means that when the TCP connection between the client and server is already open and the user fails a challenge, the server can drop the connection. Ex. 1003, ¶216. A POSITA would have known that, in 2000, HTTP relied on TCP as its primary transport layer protocol. *Id.*, ¶214.

A POSITA thus would have considered it obvious for Lim to implement the suspension of an unknown user's account by dropping or redirecting a TCP

connection established with them because Lim expressly discloses restricting users by IP address. Ex. 1003, ¶¶215-216.

The obviousness of having Lim do so is confirmed by the ubiquity of both dropping and redirecting TCP connections before the '427 Patent. Ex. 1003, ¶217. A POSITA would have understood “dropping” a TCP connection to mean that an incoming request from a user is either ignored or affirmatively rejected, which was commonly done in situations where a client is behaving maliciously, such as in response to Denial of Service (“DoS”) attacks. *Id.*, ¶218; Ex. 1020. It was similarly common to redirect TCP connections, such as by routing a user who requests a non-existent page to a “404 error” page, a frequently seen part of HTML processing. *Id.*, ¶219. Both were well-known and in common usage before the '427 Patent, allowing system designers to flexibly choose which option they wanted to use to balance system workloads against user friendliness. *Id.*, ¶220. Redirecting to an error page would be more desirable if the system designer wants real human users to have some feedback if they get a quiz wrong, whereas simply dropping the connection would be preferable if the system designer wants to limit the burden on the server. *Id.* Therefore, it would have been obvious to use either or both in implementing Lim’s invention. *Id.*

This obviousness is further confirmed by the use of IP addresses in additional prior art that, like Lim, involves determining whether an unknown user

accessing an Internet resource is a human or a bot. Ex. 1003, ¶221. For example, Lillibridge further explains how computers commonly communicated with each other over the Internet using their IP addresses and tracked client computers over multiple requests using their IP addresses. *Id.*, ¶222; Ex. 1008, 3:55-4:6, 8:35-45, 9:9-17, Fig. 1.

U.S. Patent No. 7,197,639 to Juels (Ex. 1010) further confirms the common understanding of a POSITA on suspending a user on the Internet this way. Ex. 1003, ¶223. Lim expressly discloses tracking the IP addresses of users. Ex. 1004, 13:5-14. And, like Lim, Juels discusses systems and methods for a server to address resource allocation requests from an unknown user at a client by presenting the client with a challenge. Ex. 1010, Abstract, 2:51-3:16, Figs. 1-5; Ex. 1003, ¶223. Juels explains that the unknown user's TCP connection can be dropped if they fail the challenge. Ex. 1010, 9:14-19 (puzzle protocol can "be used in conjunction with dropped connection"), 7:59-8:16, 8:27-39, Fig. 2; Ex. 1003, ¶223.

It is thus obvious to a POSITA that Lim's Internet connection would have been a TCP/IP connection, and that the most obvious way to suspend the user's account would have been to drop or redirect their TCP connection. Ex. 1003, ¶224.

To the extent Patent Owner argues that a POSITA would not have found it

obvious to implement Lim's account suspension process by dropping or redirecting the undefined originator's TCP connection, they would have found it obvious to do so in view of Lim combined with Guthrie. Ex. 1003, ¶225.

A POSITA would have been motivated to combine Lim and Guthrie for at least the reasons discussed in Section VII.E above and for Claim 8 in the following section. Ex. 1003, ¶226.

Guthrie confirms its network communications are conducted over a TCP/IP based network. Ex. 1009, 5:1-4. A POSITA implementing Lim would have been interested in limiting or restricting its number of users, and so looked to a reference like Guthrie, which explains in detail what happens when people fail an authentication. Ex. 1003, ¶227. Guthrie expressly teaches that when a user fails an authentication, the server may "return[] a failure message to the client 102 [and] the client 102 informs the user of such failure, for example, by displaying a message 'Too many incorrect passwords have been attempted, please try later.'" Ex. 1009, 9:6-10. Thus, Guthrie teaches that upon a failed challenge, its suspension includes redirecting the user's TCP connection to an error page. Ex. 1003, ¶227.

Thus, it is obvious to a POSITA that Lim's Internet connection would have been a TCP/IP connection, and the most obvious way to suspend the user's account would have been to drop or redirect their TCP connection. Ex. 1003, ¶228.

2. Claim 8

Claim 8 depends from Claim 1 and further requires “logging a source IP address of the undefined originator, and starting a timer.”

Lim renders this additional limitation obvious, both alone and in combination with Guthrie. Ex. 1003, ¶¶230-250.

As discussed above for Claim 6, Lim discloses that, when an unknown user fails a challenge, their account will be suspended, during which time processing of their requests will be stopped because they have been determined to be a robot. *See* Section VIII.A.3; Ex. 1003, ¶231; Ex. 1004, Claim 1, 9:59-67, 14:67-15:2, Fig. 5.

A POSITA would have understood that it would have been obvious for this account suspension to include logging the unknown user’s IP address. Ex. 1003, ¶232. This is particularly the case because Lim expressly discusses limiting or restricting the number of users using unique identifiers, including their IP address. *Id.*, ¶233; Ex. 1004, 5:6-6:30, 8:19-56, 13:5-14, 23:4-43, Figs. 1, 16. Thus, the most obvious way for the user to connect to the server would have been a TCP/IP connection. *Id.*

Lim also discloses tracking a particular user over time in its Figure 5 embodiment. Ex. 1004, 14:58-15:2, Fig. 5. The two most common ways of tracking users on the Web at the time were using cookies and tracking IP

addresses. Ex. 1003, ¶234. While Lim also references other identifiers including MAC addresses and CPU serial numbers, these were much less commonly used. *Id.*; Ex. 1004, 5:6-6:30, 8:19-56, 13:5-14, 23:4-43. Further, a POSITA would have readily understood that cookies would not have been desirable because they would not effectively implement Lim. *Id.* A bot could simply refuse to accept, manipulate, or delete the cookie, which would prevent applying a time period restriction. *Id.* Since Lim is designing a system to defeat malicious actors, a POSITA would have considered exactly these sorts of workarounds. *Id.* Thus, a POSITA would have turned to the obvious practice of tracking user's IP addresses, which does not have these downsides, in implementing Lim. *Id.* Indeed, an IP address must be preserved for data to be routed correctly through the Internet's TCP/IP structure. *Id.*

Additionally, because Lim also explains that this suspension should last for a time period (as discussed immediately below), it would have been obvious to log the user's IP address when their account is suspended, as that would have been the easiest and most obvious way to prevent access during that period. Ex. 1003, ¶235.

A POSITA would also have found it obvious for the unknown user's account suspension to include starting a timer. Ex. 1003, ¶236. Lim explains that, when an unknown user fails a test, their account is suspended only for a set

interval. *Id.*; Ex. 1004, Claim 1, 14:58-15:2 (on failure, “suspend[] the user’s account for a designated time interval”), Fig. 5:

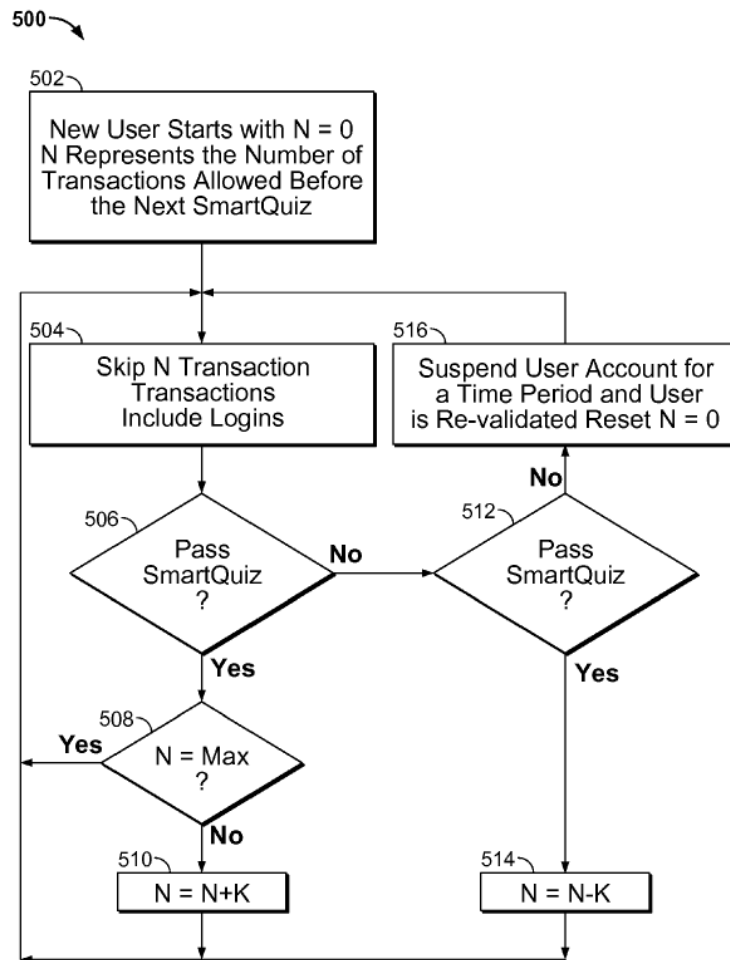


FIG. 5

See also 9:59-67.

A POSITA would have understood that, because the unknown user’s account suspension lasts for a time period, the most obvious way to do this would have been starting a timer when the user fails the challenge that triggers their suspension. Ex. 1003, ¶237. Lockout timers balance the need to allow users to

retest after an innocent failure, while preventing brute force guessing attacks. *Id.*, ¶238; *see also* Ex. 1009, 8:24-31.

The obviousness of this solution is confirmed by the extensive discussion of using timers to temporarily suspend users after failed access attempts, including in U.S. government publications dating back to the 1980s. Ex. 1003, ¶¶238-240; Ex. 1012 (Department of Defense, “Password Management Guideline,” April 1985), pp. 11-12 (“in the event of an unsuccessful login attempt, it is quite reasonable to use an internal timer to enforce the desired delay before permitting the next login attempt”); Ex. 1013 (MITRE Corp. and U.S. Air Force, “Guidelines for Designing User Interface Software,” August 1986), pp. 359-360 (“Access might be denied temporarily for some computer-imposed time interval”); Ex. 1014 (U.S. Patent No. 5,826,015 to Schmidt), 12:3-13 (lockout timer ignores IP packets to limit frequency of hostile attacks on host).

To the extent Patent Owner argues that a POSITA would not have found it obvious to implement Lim’s account suspension process by logging a source IP address of the undefined originator and starting a timer in view of Lim alone, they would have found it obvious to do so in view of Lim combined with Guthrie. Ex. 1003, ¶241.

A POSITA would have been motivated to combine Lim and Guthrie for at least the reasons discussed in Section VII.E above and those that follow. Ex. 1003,

¶242.

Guthrie teaches systems and methods for securely authenticating a client to a server over a network such as the Internet. Ex. 1009, 1:12-19, 3:53-5:15, Figs. 1A-1B; Ex. 1003, ¶243. Like Lim, Guthrie recognized that an effective networking authentication system should not simply authenticate a machine but should distinguish between legitimate human users and “a system that has been pre-programmed with access information (e.g., running a ‘script’ to permit access),” *i.e.*, between humans and bots. Ex. 1009, 1:29-37; Ex. 1003, ¶243.

Guthrie furthers this goal by implementing a “lock-out timer” that lasts for a particular duration when a user fails the authorization process. Ex. 1009, 8:10-12; Ex. 1003, ¶244. On failure, a lockout timer can be set for that user. Ex. 1003, ¶244; Ex. 1009, 12:6-9, Fig. 8B:

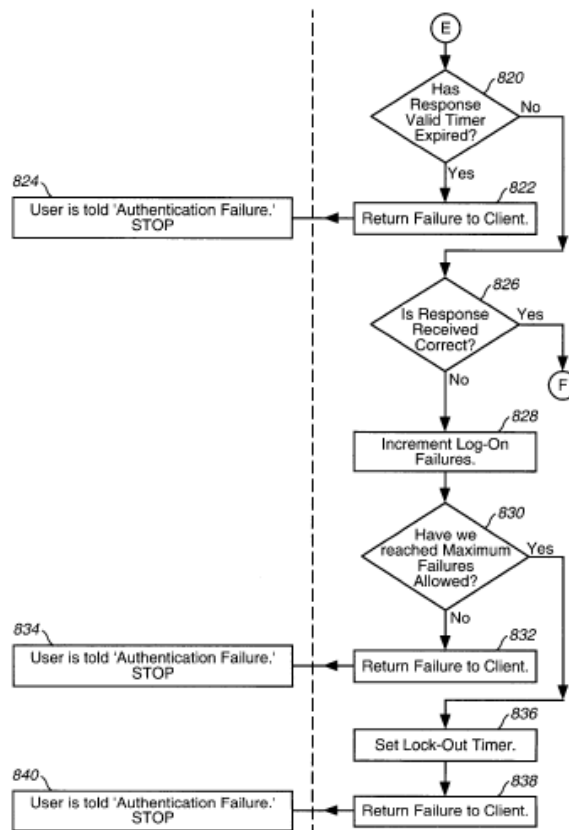


FIG. 8B

Guthrie also explains that its server “records audit information for each log-on attempt.” Ex. 1009, 13:46-47. This information can include “a date and time stamp for each log-in attempt,” “an IP address for the client 102,” and “any other information that may be determined from the authentication attempt should it represent a failure.” *Id.*, 13:47-53. Thus, Guthrie explains that, whenever an unknown user fails a log-in attempt, the server logs their source IP address and starts a timer. Ex. 1003, ¶245.

When a user attempts to access a resource, the server checks a data structure, in one embodiment user-specific account table 200, to see if lock-out timer flag

212 has been set for them. Ex. 1003, ¶246; Ex. 1009, 7:64-8:10, Fig. 6:

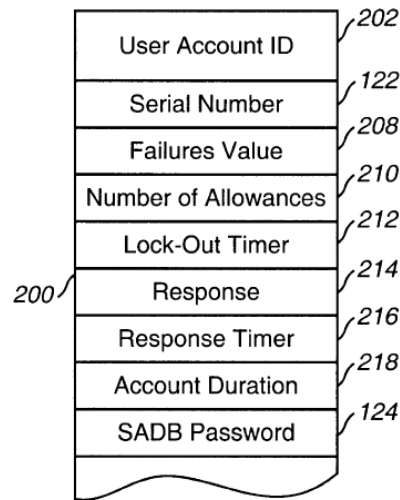


FIG. 6

If the server sees that the lockout timer has been set for this user, but has not yet expired, access is denied and the server returns a failure message to the client.

Ex. 1003, ¶247; Ex. 1009, 8:7-10, 9:6-10, 11:42-59, Figs. 7A, 8A:

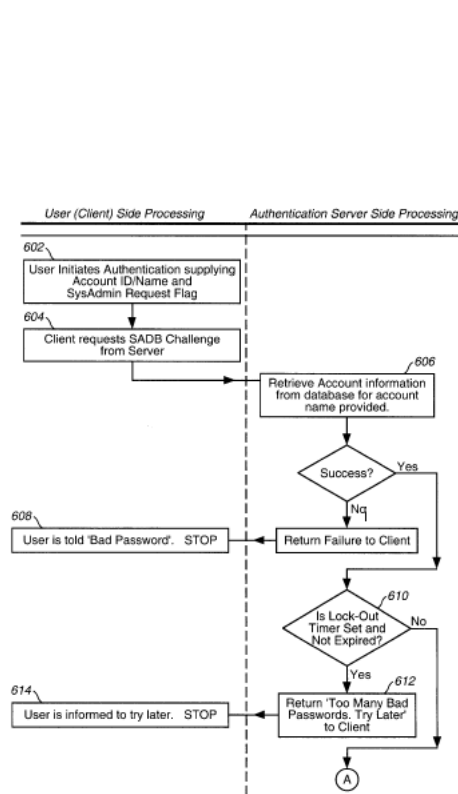


FIG. 7A

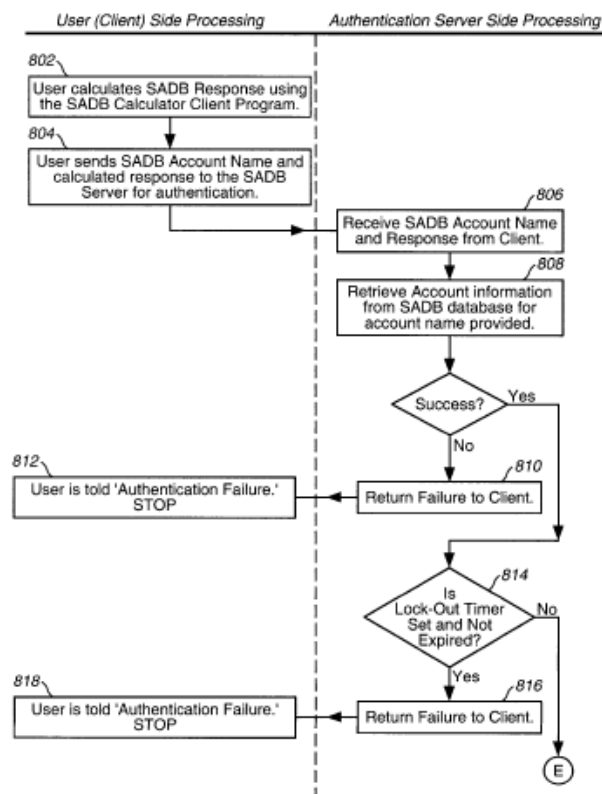


FIG. 8A

If, however, either the flag has not been set or the lockout timer has expired, authentication continues. Ex. 1003, ¶248.

Guthrie explains that it is important for its lockout timer to have a limited duration, because it prevents the user from accessing the server only for a certain amount of time, rather than banning a potentially human user forever. Ex. 1009, 8:18-23; Ex. 1003, ¶249. This way, Guthrie's lockout timer is able to both "thwart an unauthorized user from repeatedly 'hammering' the server 104 manually or through an automated application with authorization attempts," *i.e.*, prevent bots from accessing an Internet resource, and also "eventually allow[] a legitimate user

access to the server 104.” Ex. 1009, 8:24-30; Ex. 1003, ¶249.

Guthrie thus recognizes the benefits of locking out an unknown originator that fails an Internet access request only for a specified time period, rather than permanently. Ex. 1003, ¶250. Particularly given that Lim expressly discusses suspending user accounts for set time intervals, a POSITA would have considered it obvious to apply that teaching to Lim’s account suspension procedures. *Id.*; *see also* Ex. 1004, 14:67-15:2, Fig. 5. To the extent a POSITA reading Lim’s concise disclosure, which is at least as extensive as the ’427 patent’s, needed additional detail to implement Lim’s suspension time period, Guthrie provides that detail. *Id.*; Ex. 1001, 4:13-16; 4:24-34. The fact that Lim and Guthrie are both directed to effectively distinguishing humans from bots among unknown users attempting to access an Internet resource would have further motivated this combination. *Id.*; Ex. 1004, 9:46-67, 13:15-28; Ex. 1009, 1:29-37, 8:18-30. Applying Guthrie’s lockout timer to Lim would allow Lim to accomplish this goal more effectively and flexibly, as legitimate human users will not be blocked out of the server permanently. *Id.*

3. Claim 9

Claim 9 depends from Claim 1 and further requires “receiving a new request; determining whether a source IP address of the new request matches the logged source IP address of the undefined originator; determining whether said

timer is expired; and upon the source IP address of the new request matching the logged source IP address of the undefined originator and the timer being expired, responding to the new request with a second challenge that prompts a response to the second challenge.”

Lim renders this additional limitation obvious, both alone and in combination with Guthrie. Ex. 1003, ¶¶252-260.

As discussed above for Claim 6, Lim discloses that, when an unknown user fails a challenge, their account will be suspended, during which time processing of their requests will be stopped because they have been determined to be a robot. See Section VIII.A.3; Ex. 1003, ¶253; Ex. 1004, Claim 1, 9:59-67, 14:67-15:2, Fig. 5.

And as discussed above for Claim 8, a POSITA would have understood that because Lim discusses both the unknown user’s IP address and many conventional uses of IP addresses, it would have been obvious for this account suspension procedure to include logging the unknown user’s IP address. See Section VIII.C.2; Ex. 1003, ¶254; Ex. 1004, 5:6-6:30, 8:19-56, 13:5-14, 23:4-43, Figs. 1, 16. Because Lim explains that when an unknown user fails a challenge, their account suspension lasts for a set interval, a POSITA would have also found it obvious to use a timer to measure that interval, starting when the user fails their challenge. *Id.*; Ex. 1004, Claim 1, 14:58-15:2, Fig. 5.

A POSITA would also have understood that, upon receipt of a new request, it would have been obvious for Lim to determine whether the source IP address of the new request matches the logged source IP address of the suspended undefined originator and present them with a new challenge if the timer measuring their suspension has expired. Ex. 1003, ¶255. This must be the case, because otherwise Lim would have no way of determining that the interval that user is suspended for (as discussed immediately below) had passed or not. *Id.* Similarly, if Lim did not issue a new challenge after their suspension ends, Lim's disclosure of suspending the user only for a particular time period would not make sense. *Id.*

As Lim explains, once the interval the user was set to be suspended for has passed, that user is presented with a "second" or "next" challenge. Ex. 1003, ¶256; Ex. 1004, Claim 1, 14:58-15:2 ("As each quiz is taken (step 506) a determination is made as to whether the user passed the test...If the user fails a test, a retest might be offered (step 512)...Failing the retest (step 516) suspends the user's account for a designated time interval or causes some other penalty"), Fig. 5:

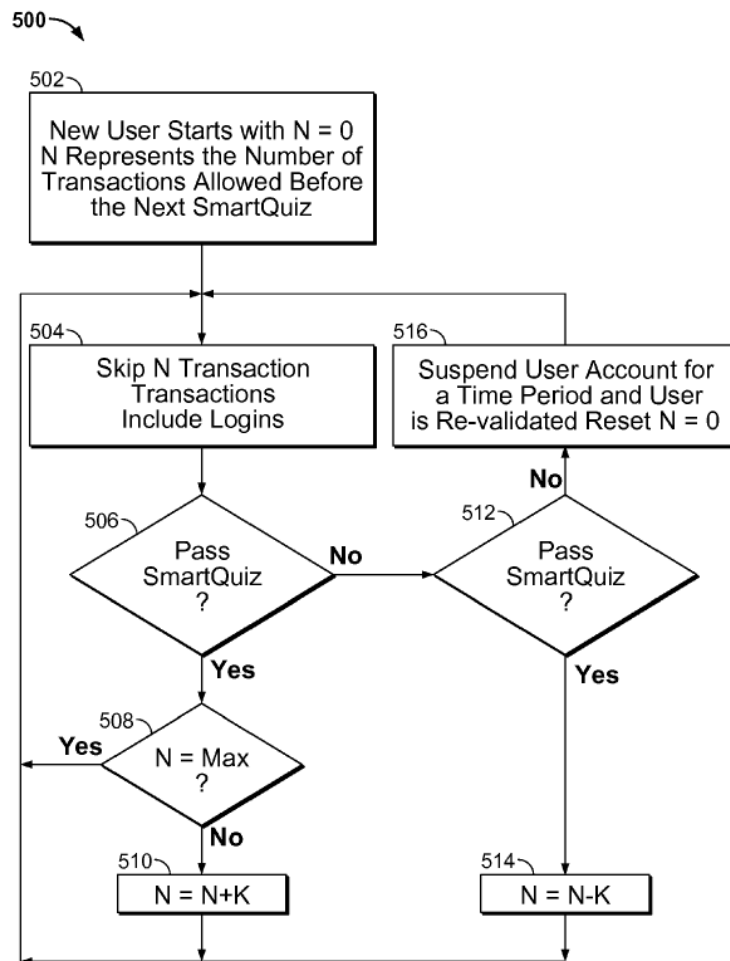


FIG. 5

See also 9:59-67.

It would thus be obvious for Lim's second challenge in response to a new request to be provided after the same user's suspension interval has passed (*i.e.*, when the source IP of a new request matches the logged source IP address of the undefined originator after their timer has expired). Ex. 1003, ¶257.

To the extent Patent Owner argues that a POSITA would not have found it obvious to modify Lim's account suspension procedures in this manner in view of

Lim alone, they would have found it obvious to do so in view of Lim combined with Guthrie. Ex. 1003, ¶258.

As explained above, a POSITA would have considered it obvious to apply Guthrie's teaching of the benefits of a lockout timer to Lim's account suspension procedures and would have been motivated to make that combination. See Section VIII.C.2; Ex. 1003, ¶259.

Guthrie teaches that, whenever an unknown user fails a log-in attempt, the server logs their source IP address and starts a timer. Section VIII.C.2; Ex. 1003, ¶260; Ex. 1009, 13:46-62. When a user attempts to access an Internet resource, the server checks to see if a lockout timer has been set for that user and, if so, if it has expired. Section VIII.C.2; Ex. 1003, ¶260; Ex. 1009, 7:64-8:10, 11:42-49, Figs. 6, 7A, 8A. If the lockout timer for that user has expired, the authentication process can continue, and the user may participate in a new log-in attempt. *Id.* A POSITA would have found it obvious to apply this teaching to Lim's account suspension procedures to fully take advantage of the benefits of Guthrie's lockout timer. *Id.* This would ensure that users failing a request are suspended only for a specified time period, rather than permanently, furthering Lim's goal of distinguishing humans from bots more effectively and flexibly. *Id.*

4. Claim 17

Claim 17 depends from Claims 11 and 16. The additional limitation of

Claim 17 is the same as that of Claim 7. Thus, Claim 17 is obvious over Lim alone, and Lim in combination with Guthrie, for the same reasons discussed above for Claim 7. See Section VIII.C.1; Ex. 1003, ¶¶261-262.

5. Claim 18

Claim 18 depends from Claim 11. The additional limitation of Claim 18 is the same as that of Claim 8. Thus, Claim 18 is obvious over Lim alone, and Lim in combination with Guthrie, for the same reasons discussed above for Claim 8. See Section VIII.C.2; Ex. 1003, ¶¶263-264.

6. Claim 19

Claim 19 depends from Claim 11. The additional limitations of Claim 19 are the same as those of Claim 9. Thus, Claim 19 is obvious over Lim alone, and Lim in combination with Guthrie, for the same reasons discussed above for Claim 9. See Section VIII.C.3; Ex. 1003, ¶¶265-266.

IX. SECONDARY CONSIDERATIONS

Petitioner is not aware of any secondary considerations that would overcome the strong showing of obviousness provided by the Petition. Ex. 1003, ¶267. Further, any attempt by Patent Owner to rely on alleged secondary considerations cannot overcome the showing of obviousness detailed above. *Tokai Corp. v. Easton Enters., Inc.*, 632 F.3d 1358, 1370 (Fed. Cir. 2011).

X. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests the Board institute review of the '427 patent and cancel all Challenged Claims.

Inter Partes Review

United States Patent No. 9,148,427

Date: March 14, 2025

Respectfully submitted,

By: /Richard F. Martinelli/

Richard F. Martinelli (Reg. No. 52,003)

Orrick, Herrington & Sutcliffe LLP

51 West 52nd Street

New York, NY 10019-6142

Telephone: (212) 506-3702

RFMPTABDocket@orrick.com

Counsel for Petitioner

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,148,427 PURSUANT TO 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 complies with the type volume limitation in 37 C.F.R. § 42.24(a)(1). According to the utilized word-processing system's word count, the petition—excluding the caption, table of contents, a table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, or listing of exhibits, and claim listing—contains 13,780 words.

Dated: March 14, 2025

By: /Richard F. Martinelli/

Richard F. Martinelli (Reg. No. 52,003)
Orrick, Herrington & Sutcliffe LLP
51 West 52nd Street
New York, NY 10019-6142
Telephone: (212) 506-3702
RFMPTABDocket@orrick.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby confirms that the foregoing PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,148,427 PURSUANT TO 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 and associated Exhibits 1001-1020 were caused to be served on March 14, 2025 via overnight courier upon the following counsel of record for Patent Owner:

27683 - Haynes and Boone, LLP
IP Section
2801 N. Harwood St.
Suite 2300
Dallas, TX 75201
United States
Re: Arkose Labs Holdings, Inc.; U.S. Patent No. 9,148,427

Courtesy copies were also served via email on Patent Owner's counsel of record in a related district court litigation styled *Arkose Labs Holdings, Inc. v. DataDome*, No. 1:23-cv-01467-RGA (D. Del.):

Christian E. Mammen
WOMBLE BOND DICKINSON (US) LLP
50 California Street, Suite 2750
San Francisco, CA 94111
Tel.: 415-433-1900
Chris.Mammen@wbd-us.com

/ Richard F. Martinelli /
