

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. 7,373,510

Original Issue Date: May 13, 2008

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

Case No. IPR2025-00693

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,373,510
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	2
A.	37 C.F.R. § 42.8(b)(1): Notice of Real Parties-in-Interest.....	2
B.	37 C.F.R. § 42.8(b)(2): Notice of Related Matters.....	2
C.	37 C.F.R. § 42.8(b)(3) and (4): Notice of Counsel and Service Information.....	3
D.	Fee for Inter Partes Review	4
III.	REQUIREMENTS FOR IPR.....	4
A.	§ 42.104(a): Grounds for Standing.....	4
B.	§ 42.104(b): Identification of Challenge	4
1.	§ 42.104(b)(1): Challenged Claims	4
2.	§ 42.104(b)(2): The Prior Art and Statutory Grounds	4
3.	Level of Ordinary Skill in the Art.....	7
4.	§ 42.104(b)(5): Evidence Supporting Challenge	7
IV.	INSTITUTION SHOULD BE GRANTED	8
A.	There Are No Grounds for a § 314 Discretionary Denial	8
B.	Denial Under § 325(d) Would Be Inappropriate.....	9
V.	TECHNOLOGY BACKGROUND.....	9
VI.	THERE EXISTS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE	13
A.	Problem Addressed by the '510 Patent and the Alleged Invention.....	14

B. Prosecution History	17
C. Claim Construction.....	18
VII. THE PRIOR ART.....	19
A. Lillibridge	19
B. Lim.....	22
C. Motivation to Combine Lim and Lillibridge	24
D. Guthrie	25
E. Motivation to Combine Lim and Guthrie.....	28
F. Motivation to Combine Lim and Guthrie with Lillibridge	31
VIII. THE CHALLENGED '510 PATENT CLAIMS ARE UNPATENTABLE OVER THE PRIOR ART.....	32
A. GROUND 1: Claims 1, 2, 7, 8, 13-15, 17-22, and 25-30 Are Obvious Over Lim In Combination With Guthrie	32
1. Independent Claim 1	32
2. Independent Claim 20	51
3. Claims 2 and 21.....	52
4. Claims 13, 22, 25-26, and 29	53
5. Claims 7, 14, 17, 27, and 30	54
6. Claims 8, 15, 18, and 19	55
7. Claim 28.....	56
B. GROUND 2: Claims 3-6, 9-12, 16, and 23-24 Are Obvious Over Lim In Combination With Guthrie In Further View of Lillibridge	57
1. Claims 3, 9, and 23.....	58

Inter Partes Review

United States Patent No. 7,373,510

2.	Claims 4, 10, and 24	65
3.	Claims 5, 6, 11, and 12	66
4.	Claim 16.....	66
IX.	SECONDARY CONSIDERATIONS	66
X.	CONCLUSION	67

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	8
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	5
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	18
<i>Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	8
<i>Tokai Corp. v. Easton Enters., Inc.</i> , 632 F.3d 1358 (Fed. Cir. 2011)	66
<i>Toyota Motor Corp. v. Cellport Sys., Inc.</i> , IPR2015-00633, Paper 11 (PTAB Aug. 14, 2015)	18
Statutes	
35 U.S.C. §§ 311-319	1
35 U.S.C. § 103	7
35 U.S.C. § 314	8
35 U.S.C. § 325	9
Rules and Regulations	
37 C.F.R. § 42	1-7
Office Patent Trial Practice Guide, 77 Fed. Reg. 48759	2

LISTING OF EXHIBITS

Exhibit	Description
1001	U.S. Patent No. 7,373,510 (the “’510 patent”)
1002	Prosecution History of U.S. Patent No. 7,373,510
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. 5,826,015 (“Schmidt”)
1011	Department of Defense, “Password Management Guideline”
1012	MITRE Corp. and U.S. Air Force, “Guidelines for Designing User Interface Software”

CHALLENGED CLAIM LISTING

Claim	Limitation No.	Limitation
1	[1-PRE]	A method for preventing robots from browsing a Web site beyond a welcome page, said method in said Web site comprising the steps of:
	[1-A]	receiving an initial request from an undefined originator and responding to said initial request with a challenge that prompts a response from said undefined originator; and receiving a response from said undefined originator and
	[1-B]	checking said response to determine whether said challenge is fulfilled; and if said challenge is fulfilled: processing any further requests; and if said challenge is not fulfilled: stopping processing of any further requests,
	[1-C]	wherein said step of stopping processing of said further requests includes the further step of: dropping or redirecting a TCP connection established with said undefined originator

Claim	Limitation No.	Limitation
	[1-D]	logging a source IP address of said undefined originator and starting a timer, further including steps upon receiving a new request of: checking whether a source IP address of said new request matches said logged source IP address; and if said source IP address matches said logged source IP address: checking whether said timer has expired and, if said timer is expired, resetting said logged IP address; and proceeding normally with said new request; and if said timer is not expired, dropping or redirecting said TCP connection; if said source IP address does not match said logged source IP address, proceeding normally with said new request and executing all the above steps with each newly received request.
2	2	The method according to claim 1 wherein: said challenge includes prompting said undefined originator to perform a specific action.
3	3	The method according to claim 2 wherein: said prompting is different at each subsequent access of said web site.
4	4	The method according to claim 3 wherein: said response includes making a choice among a plurality of prompted response options.
5	5	The method according to claim 4, wherein said response includes an answer to a quiz.
6	6	The method according to claim 3, wherein said response includes an answer to a quiz.

Claim	Limitation No.	Limitation
7	7	The method according to claim 2, wherein said response includes an answer to a quiz.
8	8	The method according to claim 2, wherein said response is suggested by textual meaning.
9	9	The method according to claim 1 wherein: said prompting is different at each subsequent access of said web site.
10	10	The method according to claim 9 wherein: said response includes making a choice among a plurality of prompted response options.
11	11	The method according to claim 10, wherein said response includes an answer to a quiz.
12	12	The method according to claim 9, wherein said response includes an answer to a quiz.
13	13	The method according to claim 1 wherein: said response includes making a choice among a plurality of prompted response options.
14	14	The method according to claim 13, wherein said response includes an answer to a quiz.
15	15	The method according to claim 13, wherein said response is suggested by textual meaning.
16	16	The method according to claim 9, wherein said response is suggested by textual meaning.
17	17	The method according to claim 1, wherein said response includes an answer to a quiz.

Claim	Limitation No.	Limitation
18	18	The method according to claim 17, wherein said response is suggested by textual meaning.
19	19	The method according to claim 1, wherein said response is suggested by textual meaning.
20	[20-PRE]	A computer process for preventing robots from browsing a web site beyond a welcome page, comprising computer-executable steps of:
	[20-A]	receiving an initial request from an undefined originator and responding to said initial request with a challenge that prompts a response from said undefined originator; and receiving a response from said undefined originator and
	[20-B]	checking said response to determine whether said challenge is fulfilled; and if said challenge is fulfilled: processing any further requests; and if said challenge is not fulfilled: stopping processing of any further requests,
	[20-C]	wherein said step of stopping processing of said further requests includes the further step of: dropping or redirecting a TCP connection established with said undefined originator

Claim	Limitation No.	Limitation
	[20-D]	logging a source IP address of said undefined originator and starting a timer, further including computer-executable steps for: checking whether a source IP address of said new request matches said logged source IP address; and if said source IP address matches said logged source IP address: checking whether said timer has expired and, if said timer is expired, resetting said logged IP address; and proceeding normally with said new request; and if said timer is not expired, dropping or redirecting said TCP connection; if said source IP address does not match said logged source IP address, proceeding normally with said new request and executing all the above steps with each newly received request.
21	21	A computer process according to claim 20, further including computer-executable steps for: prompting said undefined originator to perform a specific action.
22	22	A computer process according to claim 21, further including computer-executable steps for: prompting said undefined originator to make a response chosen from among a plurality of prompted response options.
23	23	A computer process according to claim 20, further including computer-executable steps for: changing said prompting at each access of said website.
24	24	A computer process according to claim 23, further including computer-executable steps for: prompting said undefined originator to make a response chosen from among a plurality of prompted response options.

Claim	Limitation No.	Limitation
25	25	A computer process according to claim 20, further including computer-executable steps for: prompting said undefined originator to make a response chosen from among a plurality of prompted response options.
26	26	A computer process according to claim 20, further including computer-executable steps for: prompting said undefined originator to make a response chosen from among a plurality of prompted response options.
27	27	A computer process according to claim 20, further including computer-executable steps for: prompting said undefined originator to make a response that is an answer to a quiz.
28	28	A computer process according to claim 20, further including computer-executable steps for: prompting said undefined originator to make a response based upon the knowledge content of said prompt.
29	29	The method according to claim 2 [sic] wherein: said response includes making a choice among a plurality of prompted response options.
30	30	The method according to claim 29, wherein said response includes an answer to a quiz.

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 1-30 (“Challenged Claims”) of U.S. Patent No. 7,373,510 (the “’510 patent”).

The ’510 patent describes and claims a generic process for distinguishing whether an unknown website visitor is a human or a bot using a challenge question or quiz, plus the well-known security concept of applying a lockout timer to a user after a failed challenge. Ex. 1001, Abstract.

As shown by Lim (Ex. 1004) and Lillibridge (Ex. 1008), the concept of distinguishing humans from bots through the use of a quiz/challenge question that is easy for humans to solve, but difficult for bots or other automated agents, was known for years prior to the filing of the ’510 patent. *See, e.g.*, Ex. 1004, Abstract, 2:32-38, 13:15-18, 13:40-49; Ex. 1008, 1:20-28, 2:15-18, 2:60-64. Internet users who were active in the late 1990s will recall the distorted text challenges described in Lillibridge, as what we now call CAPTCHA’s. Ex. 1008, Fig. 4; Ex. 1003, ¶¶27-29. Lim expanded on Lillibridge by, among other things, disclosing a wide variety of other quiz types beyond distorted text alone. Ex. 1004, 13:15-15:2, Ex. 1003, ¶99. These include tests for identifying images of objects, such as a yellow triangle, among a variety of shapes that human users would readily complete, but which would be challenging to computers at the time. Ex. 1004, 13:15-15:2.

Lim further taught the advantage of suspending a user from access to the site, or taking of further tests, for a time period after failing a quiz. Ex. 1004, Fig. 5, 14:58-15:2. This concept of a lockout timer is a routine technique for enhancing security of an authentication system. Ex. 1003, ¶¶36-39. As explained by Guthrie, “[t]he 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 without intervention by the system administrator.” Ex. 1009, 8:24-30.

As explained in detail below, these teachings fully disclose and render obvious the Challenged Claims. Petitioner thus 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 ’510 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 Telephone: (212) 506-3702 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 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 '510 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 '510 patent and cancel those claims as unpatentable.

1. § 42.104(b)(1): Challenged Claims

Petitioner challenges Claims 1-30 of the '510 patent.

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

The application for the '510 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

Inter Partes Review

United States Patent No. 7,373,510

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)
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, to the extent Patent Owner argues it is necessary to do so, 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 for Lim Claim 1 in all three provisional applications, as well as support for all concepts disclosed by Lim that are relied on in this Petition. Ex. 1003, Appendices B-D are charts comparing the applicable disclosures in Lim with the corresponding disclosures in each of Lim’s provisionals. *See* Ex. 1003, ¶¶76-79, 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 for Claim 1 of Lim and discloses all the concepts disclosed in Lim relied on in this Petition. Ex. 1003, ¶¶76-79, 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, ¶¶76-79, 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, ¶¶76-79, 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.*

As shown in Ex. 1003, ¶¶76-79, 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, 2, 7, 8, 13-15, 17-22, and 25-30 Are Obvious under 35 U.S.C. §103 (pre-AIA) (“Obvious”) Over Lim In Combination with Guthrie
2	Claims 3-6, 9-12, 16, 23-24 Are Obvious Over Lim In Combination with Guthrie In further view of Lillibridge

Apart from Lillibridge, none of the references on which these grounds are based were before the Examiner during prosecution of the ’510 patent.

3. Level of Ordinary Skill in the Art

A POSITA in the technology described in the ’510 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 '510 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

'510 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. *See generally* Ex. 1001.

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

V. TECHNOLOGY BACKGROUND

TCP/IP evolved from work done by DARPA in the 1960s and had become the dominant standard for Internet communications by at least the early 1990s, when it was implemented in Windows 3.1 and subsequent Windows operating systems. Ex. 1003, ¶32.

IP stands for “Internet Protocol,” and is the network layer communications protocol for relaying information over a network. *Id.*, ¶33. Each computer is assigned a numerical IP address (*e.g.*, 192.0.2.1), which is included in communications to identify both the computer and its location in the network, and thus, the path to it. *Id.* The header of each IP packet contains the IP address of

both the sending and destination computers. *Id.*

TCP stands for “Transmission Control Protocol,” and is the transport layer communications protocol. *Id.*, ¶34. TCP complements IP by operating at the layer between it and the application layer, where applications like Internet browsers operate. *Id.* While IP handles the actual delivery of data over the network, TCP communicates with the application by presenting it an abstraction of the networking details of the communication and handling transporting the data. *Id.* For example, TCP handles handshaking, and can detect and handle delivery problems, such as by requesting re-transmission of IP packets lost due to network congestion. *Id.* These technologies were foundational to the Internet and received widespread adoption along with the World Wide Web and email in the 1990s.

By 2000, a POSITA would have been very familiar with TCP/IP as the common fabric of the Internet. *Id.*, ¶35. They would have understood that reference to either of TCP or IP would also certainly mean the use of the other, especially with reference to the Web. *Id.* Accordingly, they would have understood that, when a reference discusses network communications made using IP addresses, those communications would have been ended by dropping or redirecting a TCP connection established with the undefined originator. *Id.*

Spurred by the rapid growth of the Internet, by September 2000, the field of cybersecurity was well established and built upon the decades-old understanding of

basic security principles. Ex. 1003, ¶¶27-31. The basic principles of user authentication, including using a challenge to distinguish between genuine humans and automated agents or bots using Turing Tests, were already well in place. *Id.* Indeed, the rapid growth of the web and the need to control bots was recognized and solutions that we now commonly know as CAPTCHA, which stands for “Completely Automated Public Turing Test to tell Computers and Humans Apart,” had been in use for years. *Id.*

To further supplement this bot screening technology, lockout timers have been used to balance the need to allow users to retest after an innocent failure, while also preventing malicious users from using rapid-fire, brute force attempts to guess the correct answer to the challenge. Ex. 1003, ¶36. Lockout timers solve this problem by delaying the frequency by which a system can try to gain access. *Id.* This is confirmed by several examples in other prior art references where lockout timers have been used in this way.

Indeed, this concept was repeatedly taught by the U.S. government in the 1980s. *Id.*, ¶¶36-37. For example, the Department of Defense explained that “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. The user should not be able to bypass this procedure.” Ex. 1011 (Department of Defense, “Password Management Guideline,” April 1985) at pp. 11-12; Ex. 1003,

¶37.

A MITRE Corp. and U.S. Air Force joint publication not only similarly explained that “[a]ccess might be denied temporarily for some computer-imposed time interval, or indefinitely pending review by a system administrator,” but also disclosed in detail that a system designer would want to balance the tradeoff between convenience and security in deciding the length of this suspension. Ex. 1012 (MITRE Corp. and the U.S. Air Force, “Guidelines for Designing User Interface Software,” August 1986) at pp. 359-360; Ex. 1003, ¶38. As their guidelines explained in detail:

A record of continuing failure by any particular user to complete successful LOG-ON procedures, including password entry and other tests of claimed user identity, may indicate persistent intrusion attempts. Repeated LOG-ON failures might thus be grounds for denying access to that user. Access might be denied temporarily for some computer-imposed time interval, or indefinitely pending review by a system administrator. The occasional inconvenience to a legitimate user may be tolerable in the interests of increased system security. Analysis of this tradeoff between convenience and security can determine the number and rate of LOG-ON failures that will be tolerated in any particular system application.

Id.

An additional example can be seen in U.S. Patent No. 5,826,015 to Thomas Schmidt. Ex. 1010; Ex. 1003, ¶39. Schmidt discloses ways that computers can guard against remote users that may be unauthorized. For example, for systems that can be accessed remotely, Schmidt teaches that a lockout timer 126 can be

used to limit the frequency of hostile attacks upon the host computer. Ex. 1010, 12:3-5; Ex. 1003, ¶39. Schmidt teaches that the purpose of the lockout circuitry is to “frustrate a hostile attacker who uses brute force tactics to breach the security of the desktop computer 14 by continuously submitting secure wake-up packets 42 which try all possible password combinations.” Ex. 1010, 12:5-10; Ex. 1003, ¶39. Schmidt teaches that this lockout timer can dictate when received packets from the hostile attacker can be temporarily ignored. Ex. 1010, 12:10-13; Ex. 1003, ¶39.

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

The ’510 patent aims to prevent robots (“bots”) from browsing websites by issuing a challenge to “undefined originators” accessing a site. Ex. 1001, Abstract. Successfully fulfilling the challenges results in the system assuming the user is human and failing results in an assumption the user is a robot and denial of further access. *Id.* This is the basic, prior art, CAPTCHA concept. Ex. 1003, ¶42.

As the ’510 patent explains, it was well known that bots can 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, and accessing areas not suitable for searching. Ex. 1001, 1:16-45. Solutions to “limit what the robot is allowed to do” were also known. *Id.*, 1:46-48. The ’510 patent discusses prior art solutions that “rely on cooperation from the robots” (*e.g.*, the robots.txt

protocol), which it considers as inadequate for that reason. *Id.*, 1:48-2:3.

The '510 patent also describes limiting access to registered users with passwords, which it says is “standard way ... to protect a Web site through some form of authentication.” *Id.*, 2:4-8. The patent criticizes this because it requires registration and management of the users. *Id.*, 2:8-20. Critically, the '510 patent does not acknowledge that it was also known at the time to authenticate users with tests that would be easy for humans but hard for computers, such as what we now call CAPTCHA. Ex. 1003, ¶¶44-47.

As reflected by Lim and Lillibridge, years before September 2000, the use of CAPTCHA quizzes to authenticate website users by distinguishing humans from robots was well established and built upon the longstanding understanding of basic online security principles. See Ex. 1003, ¶¶47, 27-31. 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.*

A. Problem Addressed by the '510 Patent and the Alleged Invention

The '510 patent assumes that existing systems for protecting websites required registration and management of a list of authorized users. Ex. 1001, 2:8-20; Ex. 1003, ¶48. With that framing, the patent asserts that upon “receiving an initial request from an undefined originator, the Web site responds to the request with a welcome page including a challenge.” Ex. 1001, 2:41-45; Ex. 1003, ¶49. If

the challenge is passed, the system assumes the user is human and otherwise not a robot. *Id.*, 2:45-52; Ex. 1003, ¶49. In other words, this is the basic, prior art, CAPTCHA concept. Ex. 1003, ¶¶29, 42, 65.

The claims do not focus on the disclosed pictorial challenges and, instead, claim a general challenge plus a conventional lockout timer. Ex. 1003, ¶50. Lockout timers solve a well known authentication problem of balancing the need to let users try again after a failed access, while also preventing the ability to exhaustively guess the answer to the authentication challenge or perform Denial of Service (DoS) of the authentication process. Ex. 1003, ¶¶50-55, 36-39.

Figures 3-4 of the '510 patent show the preferred embodiment of a timer that locks out users who failed their challenge for a set amount of time:

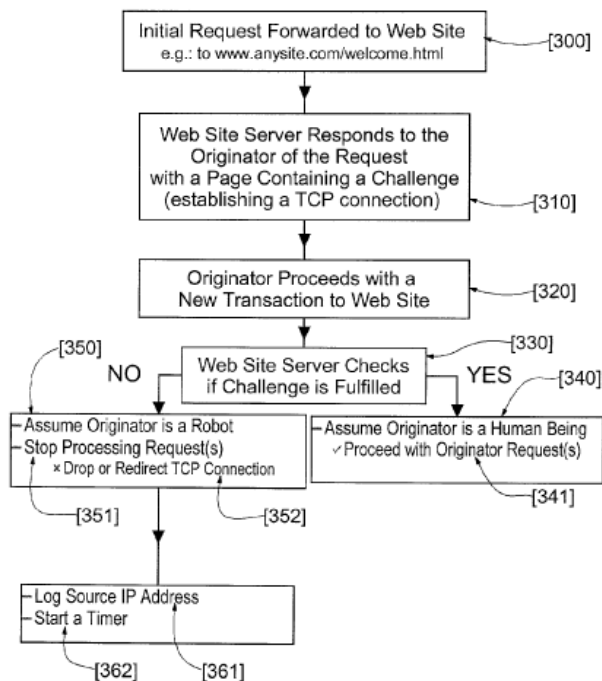


Figure 3

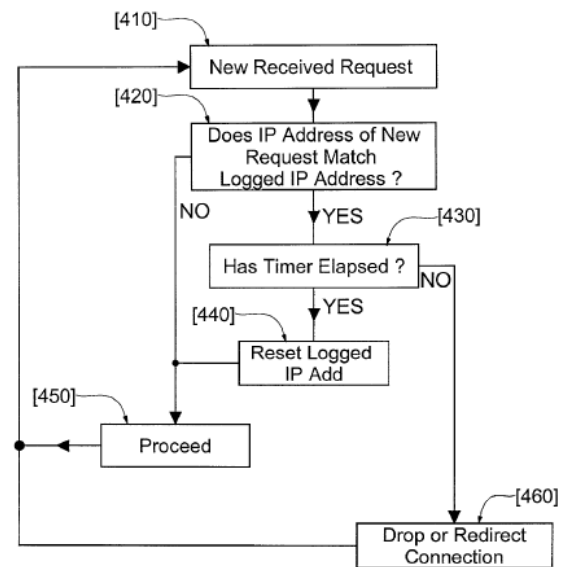


Figure 4

Ex. 1001, Figs. 3-4; Ex. 1003, ¶51.

Upon access (300), the website server challenges (310) the user. Ex. 1001, 3:59-63. If the user fails the challenge (330), they are assumed to be a robot (350), so the server stops processing their requests (351) (by dropping or redirecting their TCP connections (352)), logs their IP address (361), and starts a timer (362). Ex. 1001, 4:8-15.

Upon subsequent requests for access (410), the server checks the requestor's IP address for matches against the stored IP addresses of failed attempts (420). *Id.*, 4:16-27. If the address matches and the timer has not elapsed (430), the connection will be dropped or redirected (460). *Id.*, 4:28-29, 4:32-34. But if the

timer has elapsed (430), the user's logged IP address is reset (440) and they are allowed to attempt a new challenge (450). *Id.*, 3:28-31.

The '510 patent specification does not explain the timer at length. Ex. 1003, ¶54. It does not explain any technical implementation details of the timer, it does not explain the benefits of the timer, and it does not assert that the timer is inventive. *Id.* Rather, it simply states that the timer ensures that "access to the site may be temporarily barred, from that IP source address" because requests from the IP address are assumed to be from a robot. Ex. 1001, 4:12-21; Ex. 1003, ¶54.

In fact, the embodiment shown and described in Fig. 3-4 is the only description of the timer disclosed in the '510 patent. Ex. 1003, ¶55. Accordingly, the '510 patent assumes that the implementation of a timer would be well within the skill of a POSITA at the time. *Id.*

B. Prosecution History

The '510 patent, application No. 09/901,442, stems from foreign application EP 00480085.

On August 16, 2007, the PTO rejected all pending independent claims over Lillibridge (Ex. 1008). *See* Ex. 1002, 107-112. Specifically, the PTO found that Lillibridge disclosed a method for preventing robots from browsing a Web site by issuing a challenge to an undefined originator to either continue processing requests if the challenge is fulfilled or to drop or redirect a TCP connection if the

challenge is not. *Id.* However, the PTO found selected dependent claims allowable if rewritten in independent form. *Id.*

The applicant rewrote allowable dependent claims 6 and 32 in independent form, which generally recited the disclosed Fig. 4 lockout timer system. *See* Ex. 1002, 97-106. Specifically, claims 6 and 32 each recited the elements of the lockout timer of limitation 1[D]. *Id.*

The pending claims were allowed, without further substantive commentary from the examiner. *See id.*, 146-151 (January 9, 2008, Notice of Allowance). In other words, the claims were allegedly novel over Lillibridge because of the addition of a lockout timer, which tracked the IP address of the user to temporarily bar that source IP address on a subsequent visit to a website. However, as shown by the prior art discussed in this Petition, this concept was far from inventive at the time.

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 identifies the problem 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; Ex. 1003, ¶61. 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). Ex. 1008, 1:29-2:14; Ex. 1003, ¶62. 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.” Ex. 1008, 2:15-18; Ex. 1003, ¶62. Lillibridge criticizes prior approaches for dealing with these issues as working “only for specific contexts of a particular service” and not applicable to “any type of Web server.” Ex. 1008, 2:41-46; Ex. 1003, ¶62. 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. Ex. 1008, 2:47-59; Ex. 1003, ¶62. Lillibridge, however, criticized the use of a single flag because it would be easy to program a computer to recognize a single image. Ex. 1008, 2:47-59; Ex. 1003, ¶62.

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; Ex. 1003, ¶63. To solve these deficiencies Lillibridge proposes a server that receives a request from an unknown client and issues a “riddle” in the form of string of human-perceptible random characters that are randomly modified (*e.g.*, by visually distorting the characters or overlaying them on a visually “noisy” background such as a maze). Ex. 1008, 3:6-20; Ex. 1003, ¶63.

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:

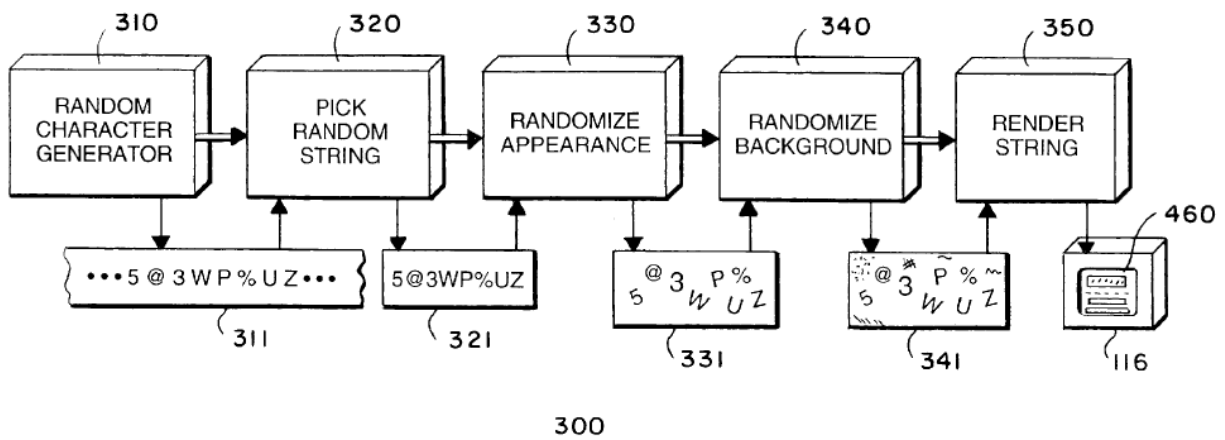
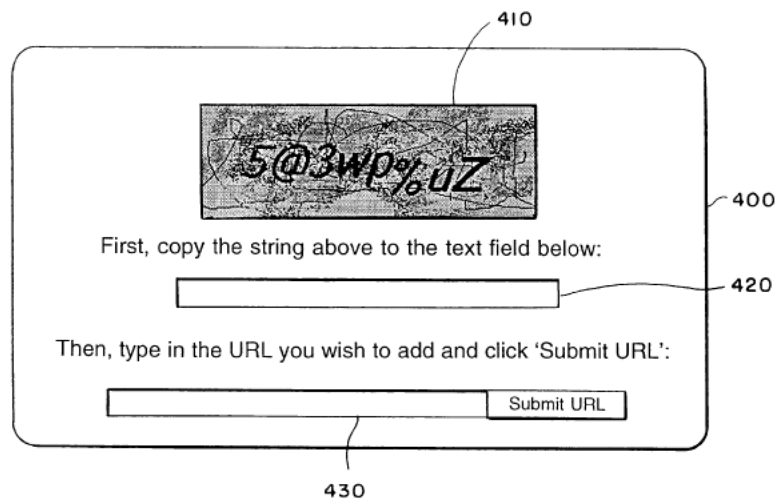


FIG. 3



The server distinguishes between a human client and an “automated agent,” based on whether the correct answer is provided. Ex. 1008, 3:21-28; Ex. 1003, ¶¶64-65. This is the basic CAPTCHA concept. Ex. 1003, ¶65.

If the correct answer is not received within a predetermined amount of time, the connection between the client and server computer is terminated by the server on the assumption that an automated agent is operating the client on behalf of the user. Ex. 1008, Abstract, 3:29-34, 6:4-6; Ex. 1003, ¶66. Lillibridge teaches that the timer is associated with a unique transaction ID or an IP address to identify the client. Ex. 1008, 8:3-5, 6-17, 27-31; Ex. 1003, ¶66.

Lillibridge represents one of several early disclosures of what we now call a CAPTCHA. Ex. 1003, ¶67. It shows that the general concept of using riddles or quizzes was already understood as early as April 1998, years before the '510

patent. Ex. 1008, (22); Ex. 1003, ¶68.

As discussed above in Section VI.B, the '510 patent's prosecution history shows the only concept claimed in the '510 patent that Lillibridge does not allegedly teach is the addition of a lockout timer. Ex. 1003, ¶69. However, Guthrie disclosed a number of embodiments of this very timer before the '510 patent. *Id.*

B. Lim

Like Lillibridge, Lim teaches systems and methods for stopping bots from accessing websites by presenting users with quiz-like challenges including various combinations of pictures and text. Ex. 1004, Abstract; Ex. 1003, ¶¶70-71. Assigned to Google, Lim represents a snapshot of some of the many ways that Google was already using what would later be coined CAPTCHA technologies to provide online security as of the filing of Lim's provisional applications in 1999 and 2000. Ex. 1004, (73); Ex. 1003, ¶¶70-71.

Lim described various challenges that combine a plurality of graphics and textual expressions instructing users to select one. Ex. 1003, ¶71. 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, *see also* Abstract. "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).” Ex. 1004, 13:15-18.

The disclosed 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 would be able to do so easily. Ex. 1004, 13:40-49; Ex. 1003, ¶72. 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, ¶¶72-73.

Lim explains that, if the unknown user succeeds at the challenge, the user will be granted access to the computer system and their further requests will be processed because they have been determined to be a human. Ex. 1004, Fig. 5, 9:59-67 (“quizzes may be introduced at various levels to thwart such automated processes and ***allow access only by live, human users***”) (emphasis added); Ex. 1003, ¶73.

Lim also expressly recognizes the value of a lockout timer and uses one in the disclosed system. Ex. 1003, ¶74. The exemplary detail about how subsequent requests can be handled in Fig. 5 includes a lockout timer suspending users for a time period after a failed quiz, at step 516. *See*, Ex. 1004, Fig. 5:

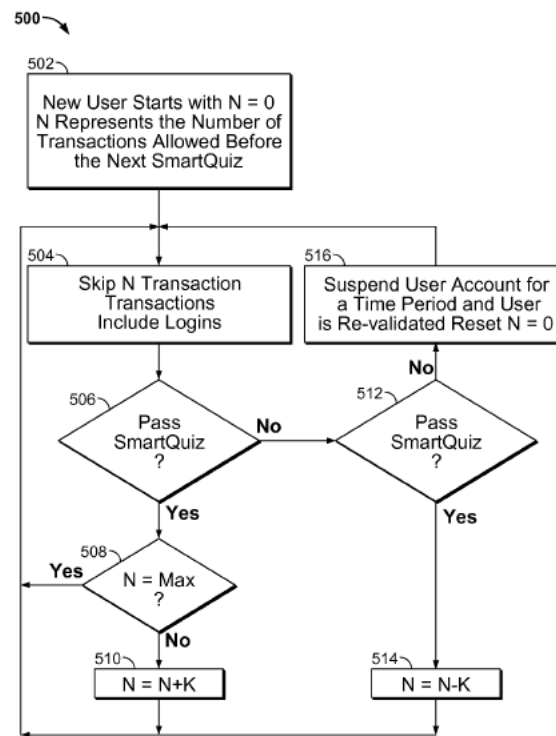


FIG. 5

As shown in Fig. 5, $N = 0$ for a new user (502), which means the user is immediately presented with a first quiz as step 504 skips N transactions, and the user is issued a challenge, quiz (506). Ex. 1004, 14:58-15:2; Ex. 1003, ¶¶74-75. If the user fails the quiz, Lim suspends the user account for a “time period” (516). See Ex. 1004, 14:65-15:2; Fig. 5 (showing that a failed smart quiz (at quiz 506 or optional retest 512) allows the system to suspend the account at step 516).

C. Motivation to Combine Lim and Lillibridge

A POSITA would have found it obvious to combine Lim and Lillibridge for many reasons. Ex. 1003, ¶80.

Lim and Lillibridge are not only part of the same field, Internet

authentication and security, they are directed to the same specific problem—distinguishing humans and bots in evaluating unknown users of websites and doing so by providing tests that would be easy for humans but difficult for bots. *See, e.g.*, Ex. 1004, Abstract, 2:32-38, 13:15-18, 13:40-49; Ex. 1008, 1:20-28, 2:15-18, 2:60-64; Ex. 1003, ¶81.

Lim and Lillibridge even expressly address this problem for the same use cases, such as preventing advertising fraud. *See, e.g.*, Ex. 1004, 13:40-51; Ex. 1008, 1:40-46; Ex. 1003, ¶82.

Further, the references are implemented using the same standard network technologies. *See, e.g.*, Ex. 1004, 1:35-2:9, 4:7-24, 5:6-7:61, 8:18-56, 23:3-43, Figs. 1, 16; Ex. 1008, 1:13-19, 2:66-3:5, 3:55-4:6, Fig. 1; Ex. 1003, ¶83. Thus, a POSITA could have predictably and successfully combined them without undue experimentation. Ex. 1003, ¶83.

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 below. Ex. 1003, ¶84. For example, a POSITA would have been inspired to combine Lillibridge's express disclosure of generating a modified riddle for each request with Lim's quizzes, to enhance Lim's security. *Id.*

D. Guthrie

Guthrie teaches the secure authentication of a client to a server over a

network such as the Internet. *See, e.g.*, Ex. 1009, 1:12-19, 3:53-5:15, Figs. 1A-1B:

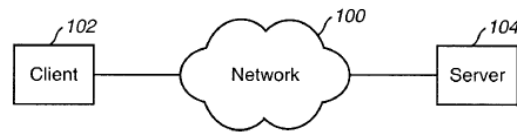


FIG. 1A

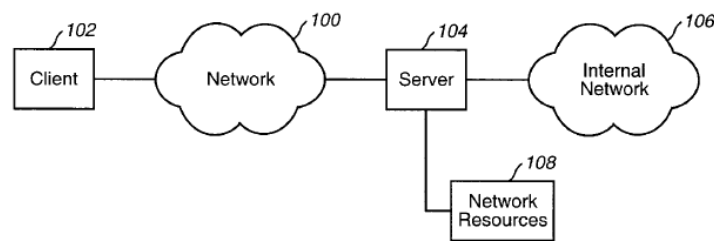


FIG. 1B

Guthrie explains that an effective network authorization should perform “user authentication, rather than simply machine or system authentication,” 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. Thus, Guthrie recognizes that automated systems (*e.g.*, bots) have capabilities that must be specifically protected against, in particular, the ability to rapidly make many attempts to defeat an authentication. Ex. 1003, ¶86.

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 without intervention by the system administrator.” *Id.*, 8:24-30 (emphasis added). Guthrie explains that the user should only be prohibited from accessing the server for a certain amount of time, so the lockout timer is set to for a particular duration. *Id.*, 8:18-23.

As implemented, the server checks the user account table 200 to see if the lock-out timer flag 212 has been set for this user. *Id.*, 7:64-8:10, Fig. 6:

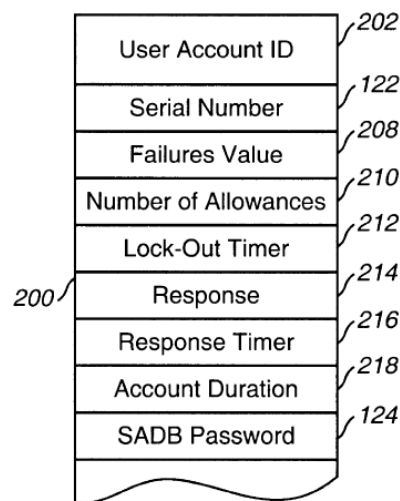


FIG. 6

If the flag 212 is set and the lockout timer has not expired, access is denied. Ex. 1009, 9:6-10. If the flag is not set or timer has expired, the authorization process continues. *Id.*, 8:7-10, 9:6-10, Fig. 7A:

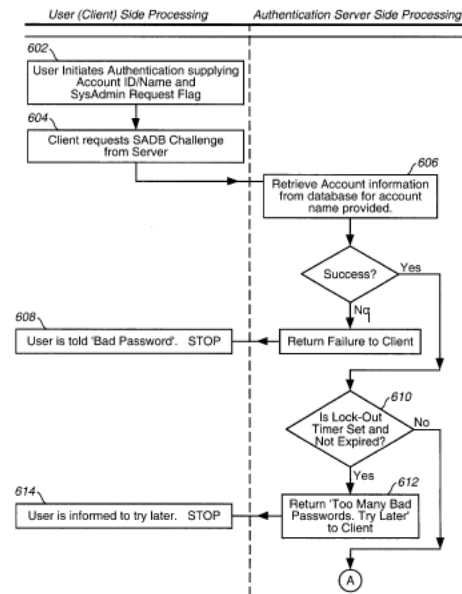


FIG. 7A

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 potentially honest error. Ex. 1009, 8:24-30; Ex. 1003, ¶¶85-91.

E. Motivation to Combine Lim and Guthrie

A POSITA would have found it obvious to combine Lim and Guthrie for many reasons. Ex. 1003, ¶92.

Lim and Guthrie—each disclosing lockout timers—are not only part of the same field, Internet authentication and security, they are directed to the same specific problem—distinguishing humans and bots in evaluating unknown users of

websites. *See, e.g.*, Ex. 1004, Abstract, 2:32-38, 13:15-18, 13:40-49, 14:68-15:2; Ex. 1009, 1:12-19, 1:29-37, 3:53-5:15, 7:64-8:18, Figs. 1A-1B; Ex. 1003, ¶93.

Further, the references are implemented using the same World Wide Web network technologies. *See, e.g.*, Ex. 1004, 1:35-2:9, 4:7-24, 5:6-7:61, 8:18-56, 23:3-43; Ex. 1009, 1:12-19, 4:50-5:15, Figs. 1A-1B; Ex. 1003, ¶94. Thus, a POSITA could have predictably and successfully combined them without undue experimentation. Ex. 1003, ¶94.

Additional details regarding why a POSITA would have been motivated to combine Lim and Guthrie to arrive at the particular claims at issue are discussed in Section VIII.B below. Ex. 1003, ¶95. For example, a POSITA would have been inspired to combine Guthrie's lockout timer with Lim's quizzes, to accomplish Lim's goal of distinguishing humans from bots among unknown users attempting to access an Internet resource more effectively and flexibly, as legitimate human users will not be blocked out of the server permanently. *Id.* Specifically, Lim contemplates that failing a test can result in the user's account being suspended for some designated time interval or causes some other penalty. Ex. 1004, 14:67-15:2, Fig. 5. To the extent a POSITA reading Lim needed additional detail on how to implement a suspension, Guthrie provides that detail. Ex. 1003, ¶95.

Guthrie provides exemplary details of how such suspension can be accomplished using a conventional lockout timer. Ex. 1009, 8:10-12, 12:6-9, Fig.

8A; Ex. 1003, ¶96. This provides a POSITA implementing the Lim system with detailed options for implementing a suspension, which Lim expressly recognized would be beneficial. Ex. 1003, ¶96.

Guthrie further explains that it is important for its lockout timer to have a limited duration, because it would be disadvantageous to ban a potential human user forever. Ex. 1009, 8:18-23; Ex. 1003, ¶97. 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 without intervention by the system administrator." Ex. 1009, 8:24-30; Ex. 1003, ¶97.

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, ¶98. A POSITA would have considered it obvious to apply that teaching to Lim's account suspension procedures. *Id.* They would have been motivated to form this combination because both Lim and Guthrie 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, ¶98; Ex. 1004, 9:46-67, 13:15-28; Ex. 1009, 1:29-37, 8:18-30.

F. Motivation to Combine Lim and Guthrie with Lillibridge

A POSITA would have similarly found it obvious to combine the system and method of Lim with the features of both Guthrie and Lillibridge because those references teach elaborations on features of Lim as well as distinct additional features that are complementary and enhance the Lim's bot detection system. Ex. 1003, ¶99. As described in Section VII.E, a POSITA would have found it obvious to combine Lim and Guthrie, for example, to take advantage of the detailed description of Guthrie's lockout timer to aid in embodying Lim's suspension time period. Ex. 1003, ¶100. And similarly, as described in Section VII.C, a POSITA would also have found it obvious to combine Lim with Lillibridge to implement Lillibridge's teaching of the importance to modify quizzes from one request to the next. *Id.*

Indeed, all three references are directed to the same specific problem—distinguishing humans and bots in evaluating unknown users of websites. *See, e.g.,* Ex. 1004, Abstract, 2:32-38, 13:15-18, 13:40-49; Ex. 1008, 1:20-28, 2:15-18, 2:60-64; Ex. 1009, 1:12-19, 1:29-37, 3:53-5:15, Figs. 1A-1B; Ex. 1003, ¶101.

Each reference is implemented using Internet and Web technologies. *See, e.g.,* Ex. 1004, 1:35-2:9, 4:7-24, 5:6-7:61, 8:18-56, 23:3-43; Ex. 1008, 1:40-46; Ex. 1009, 1:12-19, 4:50-5:15, Figs. 1A-1B; Ex. 1003, ¶102. Thus, 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 with Guthrie to arrive at the particular claims at issue are discussed in Section VIII.B below. Ex. 1003, ¶103. The POSITA would have been motivated to form this predictable combination between references 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, ¶103; Ex. 1004, 9:46-67, 13:15-28; Ex. 1008, 1:20-28, 2:15-18, 2:60-64; Ex. 1009, 1:29-37, 8:18-30.

VIII. THE CHALLENGED '510 PATENT CLAIMS ARE UNPATENTABLE OVER THE PRIOR ART

A. GROUND 1: Claims 1, 2, 7, 8, 13-15, 17-22, and 25-30 Are Obvious Over Lim In Combination With Guthrie

1. Independent Claim 1

Lim in combination with Guthrie renders Claim 1 obvious. Ex. 1003, ¶¶106-152.

a) [1-PRE]

If the preamble is limiting, Lim discloses “[a] method for preventing robots from browsing a Web site beyond a welcome page.” Ex. 1003, ¶ 107.

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 ... by using a quiz process that requires user interaction.” Ex. 1004, 2:33-39 (emphasis added), *see also, e.g.*, Abstract, 13:15-28, 8:25-30, Claim 1, Fig. 1.

Lim explains that when a user reaches the welcome page of a website, “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, ¶ 110.

b) Element [1-A]

Lim discloses “receiving an initial request from an undefined originator and responding to said initial request with a challenge that prompts a response from said undefined originator; and receiving a response from said undefined originator.” Ex. 1003, ¶¶ 111-115.

Lim’s quizzes are challenges and are issued in response to an initial request from an unknown user (*i.e.*, an undefined originator) to access a website. Ex. 1003, ¶ 112. Lim explains that it challenges new users “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” (*i.e.*, a bot). Ex. 1004, 2:33-39 (emphasis added), *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,” in order to block “robots or bots”), 13:15-28 (quizzes employed to verify undefined users—such as new users during registration, undefined users during follow-up registrations, and/or users between transactions—are humans and not bots), 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). Because these are new users, they are an undefined originator and are tested when they are accessing a website because they are making an initial request. Ex. 1003, ¶ 112.

Even further, because the intent of the challenges is to distinguish humans from bots, Lim confirms that these challenges are provided to unknown users; otherwise, there would be no need for the challenge. Ex. 1003, ¶ 113. Lim contemplates that “[*n*ew users may be referred to a service provider’s Web site ... offering a service [and b]efore being allowed to register, these *new users* may be asked to answer one or more questions of a quick to test whether they are human users or not.” Ex. 1004, 9:45-67 (emphasis added).

Finally, Lim explains that responses to these quizzes are naturally provided by the user. See Ex. 1004, 3:1-3, 14:43-45, Abstract, 2:33-39, 9:53-67, 13:15-39, Claim 1; Ex. 1003, ¶114. For example, Lim teaches that “[a] separate text box or other data entry device rendered in the web page with the quick question image

could then be used by the user to enter his/her answer.” Ex. 1004, 13:37-39, 52-56. Thus, Lim discloses “receiving a response from said undefined originator.” Ex. 1003, ¶ 114.

Lim thus receives and responds to an undefined originator’s initial request with a challenge that prompts a response from the originator and awaits the response. Ex. 1003, ¶115.

c) Element [1-B]

Lim discloses “checking said response to determine whether said challenge is fulfilled; and if said challenge is fulfilled: processing any further requests; and if said challenge is not fulfilled: stopping processing of any further requests.” Ex. 1003, ¶¶ 116-123.

After receiving the undefined originator’s response to the challenge, Lim also discloses the natural step of “checking said response to determine whether said challenge is fulfilled.” Ex. 1004, 9:64-66, Claim 1 (“determining, by the first computer system, ***whether the respective response matches its corresponding single correct and distinct response***”) (emphasis added); Ex. 1003, ¶119.

And “if said challenge is fulfilled,” Lim “process[es] any further requests.” Ex. 1003, ¶120. This naturally follows from the fact that Lim’s tests are designed, like the ’510 patent, to allow humans access, while excluding bots. *Id.* Lim explains that, if the unknown user succeeds at the challenge, the user will be

granted access to the computer system and their further requests will be processed

because they have been determined to be a human. Ex. 1004, Fig. 5, 9:59-67

(“quizzes may be introduced at various levels to thwart such automated processes and ***allow access only by live, human users***”) (emphasis added), 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***”) (emphasis added); see also Abstract, 2:32-39, 8:19-30, 9:45-59, Fig. 1; Ex. 1003,

¶120.

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

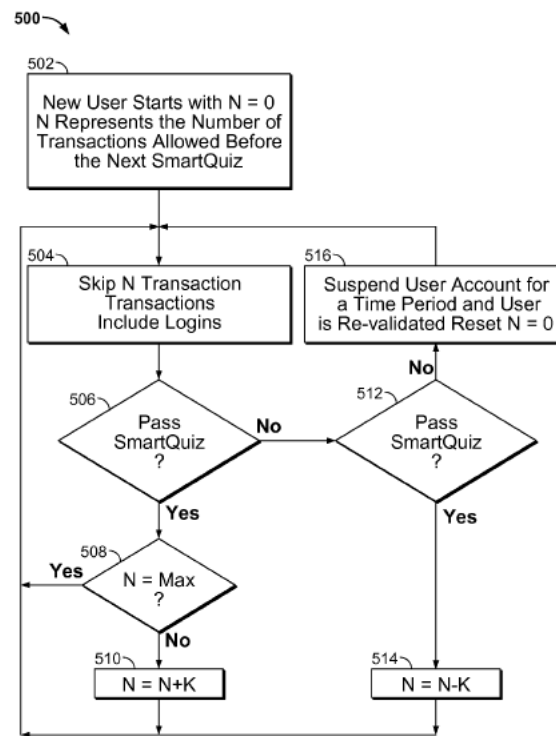


FIG. 5

As Lim shows in Fig. 5, $N = 0$ for a new user, which means the user is immediately presented with a first quiz as step 504 skips $N=0$ transactions and proceeds directly to issuing a challenge (at step 506). Ex. 1004, 14:58-15:2; Ex. 1003, ¶¶121-122. If they pass the first quiz (step 506), the user is able to engage in at least $N+K$ transactions (510) without being quizzed when the process returns to step 504. Ex. 1004, 14:58-15:2; *see also* Ex. 1003, ¶¶121-122.

Lim also discloses that “if said challenge is not fulfilled: stopping processing of any further requests.” Ex. 1003, ¶123. If the user fails the quiz, Lim dictates that access will be blocked, step 516. *See* Ex. 1004, 14:67-15:2 (“Failing the [optional] retest (step 516) suspends the user’s account for a designated time

interval or causes some other penalty”), Fig. 5 (showing that a failed smart quiz (at quiz 506 or optional retest 512) allows the system to suspend the account at step 516), 9:59-67, Claim 1 (“***otherwise, not granting the human operator access to the computer-based resource***”), Abstract, 2:32-39, 9:45-59, 14:58-67, Fig. 1; Ex. 1003, ¶123.

d) Element [1-C]

Element 1-C requires “wherein said step of stopping processing of said further requests includes the further step of: dropping or redirecting a TCP connection established with said undefined originator.”

Lim renders this additional limitation obvious, both alone and in combination with Guthrie. Ex. 1003, ¶¶124-131.

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 Ex. 1004, Claim 1, 9:59-67, 14:67-15:2, Fig. 5; Ex. 1003, ¶126.

Lim explains that its network communications are conducted over the Internet and involve communications made using IP addresses. Ex. 1003, ¶¶127; Ex. 1004, Figs. 1, 16:

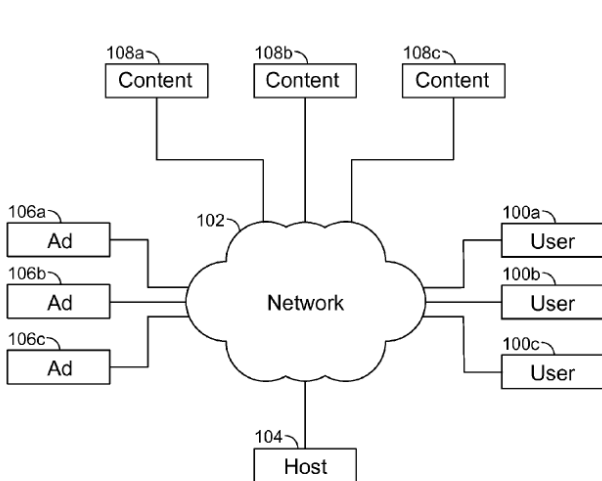


FIG. 1

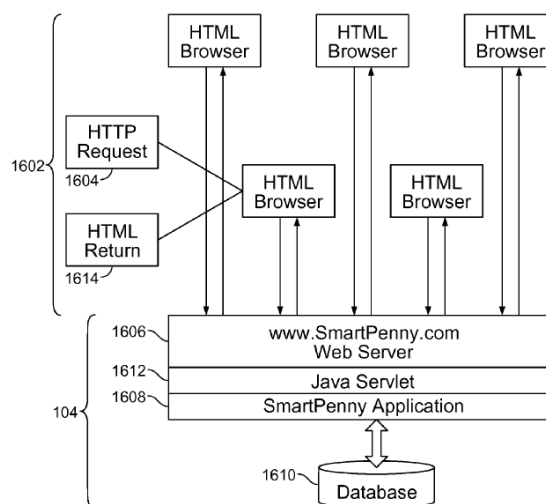


FIG. 16

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).

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. Ex. 1003, ¶128. Indeed, Website data was, and is, transferred over the Internet using a TCP/IP connection. *Id.* Thus, Lim's references to IP addresses and other related functionalities like HTTP requests would make a POSITA expect that TCP/IP would have been used. *Id.*

Lim's teaching to suspend the user obviously requires dropping or redirecting a TCP connection, which is the Web's connection interface. Ex. 1003, ¶129. This is confirmed by the discussion of 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. *Id.* In fact, Lim expressly discusses

limiting or restricting the number of users and connects this limitation or restriction to unique identifiers such as the user's IP address. *See* Ex. 1004, 13:4-14. Because the user's IP identifies the client and is part of the TCP/IP protocol, this means that when TCP connection between the client and server is already open, when the user fails a challenge, the server can drop or redirect the connection. Ex. 1003, ¶129.

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 a TCP/IP connection in view of Lim alone, they would have found it obvious to do so in view of Lim combined with Guthrie. Ex. 1003, ¶ 130. Guthrie confirms its network communications are conducted over a TCP/IP based network. Ex. 1009, 5:1-4; Ex. 1003, ¶130. If a POSITA reading Lim needed to know implementation details for limiting or restricting its number of users, Guthrie explains in detail what happens when people fail such an authentication. Ex. 1003, ¶130. For example, Guthrie expressly teaches that "[i]f the lock-out timer flag is set, and not expired, then ... the server 104 returns 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; Ex. 1003, ¶130. In other words, Guthrie teaches that upon a failed challenge and an expiration of a lockout timer, its suspension includes redirecting their TCP connection to an error page. Ex. 1003, ¶130.

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, ¶131.

e) Element [1-D]

Element 1-D requires, “[i] logging a source IP address of said undefined originator and starting a timer, further including steps upon receiving a new request of [ii] checking whether a source IP address of said new request matches said logged source IP address; and [ii.a] if said source IP address matches said logged source IP address: [iii] checking whether said timer has expired and, [iii.a] if said timer is expired, resetting said logged IP address; and proceeding normally with said new request; and [iii.b] if said timer is not expired, dropping or redirecting said TCP connection; [ii.b] if said source IP address does not match said logged source IP address, proceeding normally with said new request and executing all the above steps with each newly received request.” Ex. 1003, ¶¶132-133.

Lim renders this additional limitation—which merely verbosely describes a lockout timer where users are tracked by IP address—obvious, both alone and in combination with Guthrie. Ex. 1003, ¶134. Specifically, the claim spells out that the lockout timer gathers data (at 1-D.i, the claimed method logs IP addresses to track users that fail and associates a started timer with the logged IP address) and

enters two conditional paths for new requests: (1) the first conditional (limitation 1-D.ii) checks the new request for a logged IP address: if the IP is not logged, limitation 1-D.ii.b dictates the user faces the normal robot test, if the IP is logged limitation 1-D.ii.a requires checking the timer; (2) the second conditional is the timer check (limitation 1-D.iii): if the timer is expired, 1-D.iii.a requires treating the request normally (*i.e.*, retesting) and if the timer is not expired the lockout is enforced according to 1-D.iii.b. Ex. 1003, ¶¶132-133.

Limitation 1-D.i

Lim alone or in combination with Guthrie renders limitation 1-D.i obvious. Ex. 1003, ¶¶135-139. As discussed above for limitation 1-B, Lim discloses that, when an unknown user fails a challenge, their account will be suspended for a time period, during which time processing of their requests will be stopped, because they have been determined to be a robot. *See* Section VIII.A.1.c; Ex. 1003, ¶¶135, 116-123; Ex. 1004, Claim 1, 9:59-67, 14:67-15:2, Fig. 5. Lim also expressly discloses using IP addresses to uniquely identify and restrict users. Ex. 1004, 13:5-14 (emphasis added) (“[c]omputer systems configured in accordance with the present invention **may limit or restrict** ... users access from computers or other web-capable devices associated with certain unique identifiers such as medium access control (MAC) addresses, **IP addresses**, or central processing unit (CPU) serial numbers.”).

Lim explains that, when an unknown user fails a test, their account is suspended for a time period, which would most obviously be tracked by starting a timer. *See*, Ex. 1003, ¶136; Ex. 1004, 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, ...Failing the [test] suspends the user’s account for a designated time interval or causes some other penalty”), Fig. 5:

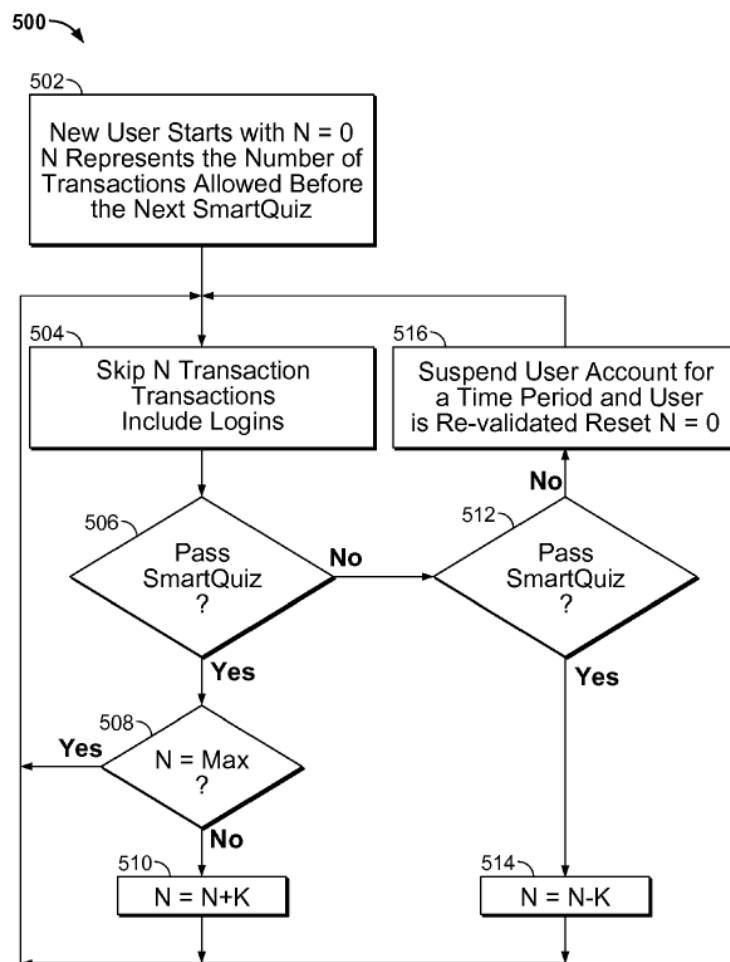


FIG. 5

See also 9:59-67. To affect the suspension for a time period, the Lim system must

record some way to track the time, *e.g.*, starting a timer. Ex. 1003, ¶136.

Moreover, because Lim discloses tracking users by IP addresses, the timer for a particular failed user would need to be associated with that user's IP address. *Id.*

Users arrive at the website at different times. *Id.* Thus, to accomplish the function of suspending a particular failed user for its specific time period, the Lim system would associate a timer specific to the failed user. *Id.* A POSITA would have understood that Lim's suspension of a User Account for a time period (Fig. 5) would be done advantageously by logging an IP address of the user and associating it with a timer. *Id.* Finally, to enforce the suspension time period, Lim's system would need to check the IP address of the new request to see if they matched any of the logged IP addresses currently subject to a suspension timer. *Id.* If Lim did not do so, there would be no way to distinguish suspended IP addresses from those that are free to use the system. *Id.*

A POSITA implementing Lim would have further confirmed the obvious solution of logging an IP address and starting a timer, in view of Guthrie. Ex. 1003, ¶ 137. 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. *Id.*

Guthrie details how to implement a "lock-out timer" that lasts for a particular duration when a user fails the authorization process. Ex. 1009, 8:10-12, 1:12-19, 29-37, 3:53-5:15, Figs. 1A-1B; Ex. 1003, ¶138. Specifically, if an

unknown user fails the authorization process, a lockout timer can be set for them.

Ex. 1003, ¶138; Ex. 1009, 12:6-9 (describing that as shown in Fig. 8B, if the maximum number or set of failures has been reached, then in step 836, the server 104 initiates the lockout timer by setting the lock-out timer record 212), Fig. 8B:

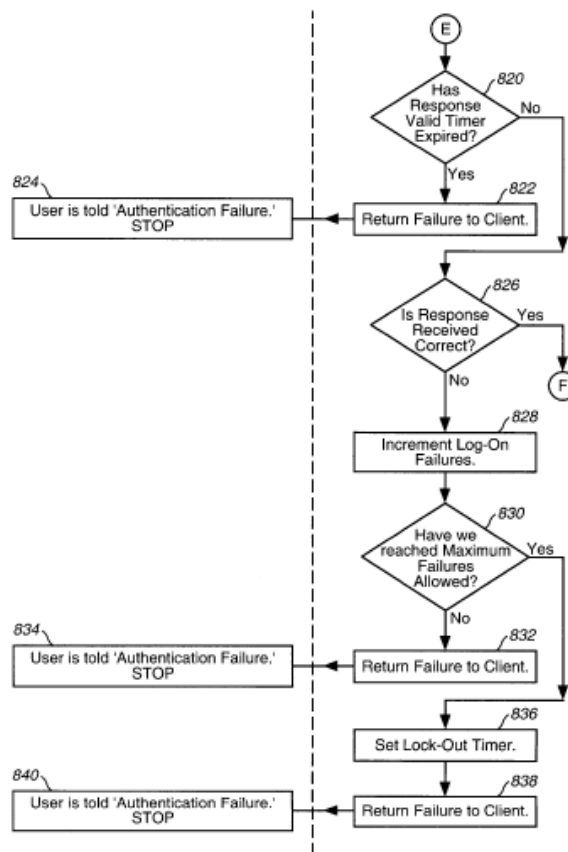


FIG. 8B

Guthrie 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.” Ex. 1009, 13:47-62. Thus, Guthrie expressly explains that,

whenever an unknown user fails a log-in attempt, the server logs their source IP address and starts a timer. Ex. 1003, ¶139.

Limitation 1-D.ii.a and 1-D.ii.b

Lim alone or in combination with Guthrie renders limitations 1-D.ii.a and 1-D.ii.b obvious. Ex. 1003, ¶140. As discussed above, Lim discloses tracking users by IP address and suspending them for a time period. Ex. 1003, ¶141. To enforce its suspension, a POSITA would understand that Lim's system requires checking the IP addresses of new requests and enforcing controls if the IP address of the new request matches a logged IP address. Ex. 1003, ¶141. If Lim did not check the IP addresses of new requests, it would have no way to determine whether the new requestor is subject to a lockout timer. *Id.* Of course, if the IP address is not logged, the user is a truly new user and will be treated accordingly, which would involve starting normal bot test processing, as reflected for example in Lim's step 502 of Fig. 5. Ex. 1003, ¶141; Ex. 1004, 14:58-15:2. On the other hand, if the user's IP address is logged, enforcing the time period suspension of step 516 would require checking the timer associated with the user's IP address. Ex. 1003, ¶141; Ex. 1004, 14:58-15:2.

A POSITA's understanding of how to handle this first conditional branch would be informed by Guthrie, which, as explained above, discloses logging IP addresses. Ex. 1009, 13:47-53; Ex. 1003, ¶142. Using that stored information,

Guthrie's server checks the user account table 200 to see if the lock-out timer flag 212 has been set when a user attempts to access a resource. Ex. 1003, ¶142; Ex. 1009, 7:64-8:10; 11:42-49, Figs. 6, 7A, 8A:

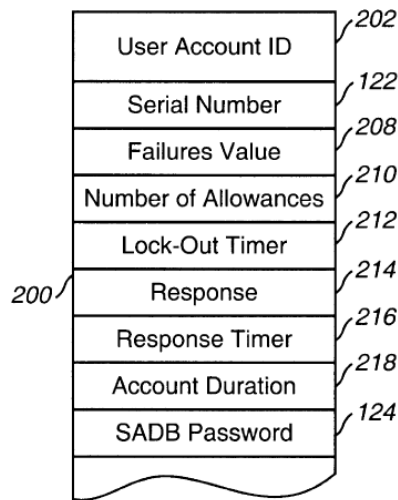


FIG. 6

Specifically, “the server 104 determines whether a lock-out timer flag is active by reading a lock-out timer record 212 in the user account table 200,” which record 212 includes both a lock-out timer flag and the timer that is started, as recited in limitation ii.a. Ex. 1003, ¶143; Ex. 1009, 8:7-16. This is further discussed below with reference to conditionals iii.a and iii.b. Of course, if the user is not logged, they would be treated like a new user and processed normally, as recited in limitation ii.b.

For the reasons above, Lim alone or in combination with Guthrie render obvious, “if said source IP address matches said logged source IP address:

checking whether said timer has expired if said source IP address does not match said logged source IP address, proceeding normally with said new request and executing all the above steps with each newly received request.” Ex. 1003, ¶144.

Limitations 1-D.iii.a and 1-D.iii.b

If the IP check reveals the new request is from a logged IP address (1-D.ii), Lim alone or in combination with Guthrie renders obvious the further conditional steps of describing what happens whether or not the timer is expired, as recited in limitations 1-D.iii.a and 1-D.iii.b. Ex. 1003, ¶145.

At step 516 of Fig. 2, Lim discloses suspending the user account for a time period after which N is reset to 0. Ex. 1003, ¶146.

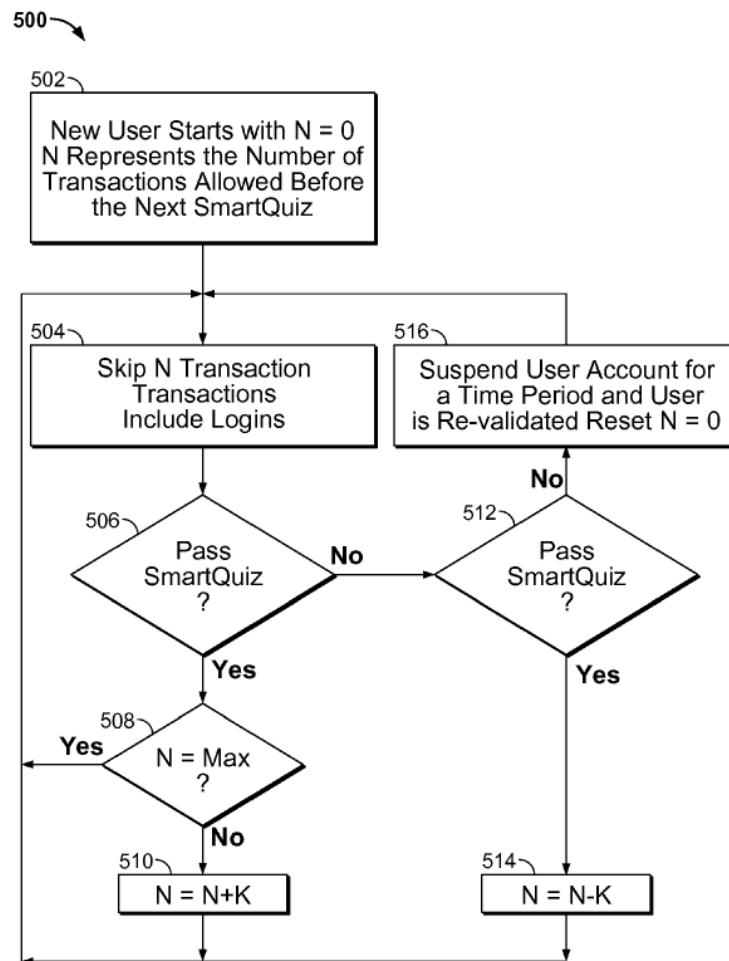


FIG. 5

As shown above, after the suspension (*i.e.*, the timer is expired) the flow out of step 516 lead to step 504 and “proceed[s] normally with said new request.” *Ex.* 1003, ¶¶147. Moreover, because $N = 0$ is the same condition as for a completely new user (compare, step 502), the logging will be reset. *Id.* Thus, Lim renders limitation 1-D.iii.a obvious. *Id.*

Lim’s disclosure of suspending the user for a time period also renders obvious limitation 1-D.iii.b’s requirement that the user TCP connection is dropped

or redirected if the time is not expired. Ex. 1003, ¶148. Because Lim's system is built for the Web, which employs TCP/IP, enforcement of Lim's suspension would most naturally be accomplished by dropping or redirecting the user's TCP connection. *Id.*

This understanding of a POSITA would have been further confirmed and enhanced by Guthrie. Guthrie's Figs. 7A / 8A below show that if the server sees that the lockout timer has been set for this user but has not yet expired (at steps 810 and 814), access is denied and the server **redirects** the client to an authentication failure screen. Ex. 1003, ¶149; Ex. 1009, Figs. 7A, 8A, 8:7-10, 9:6-10, 11:42-59.

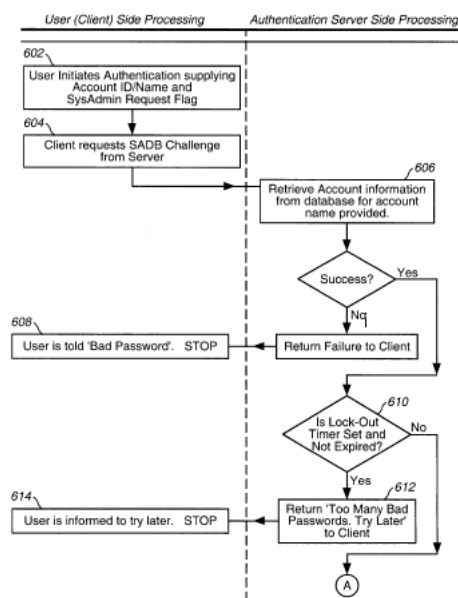


FIG. 7A

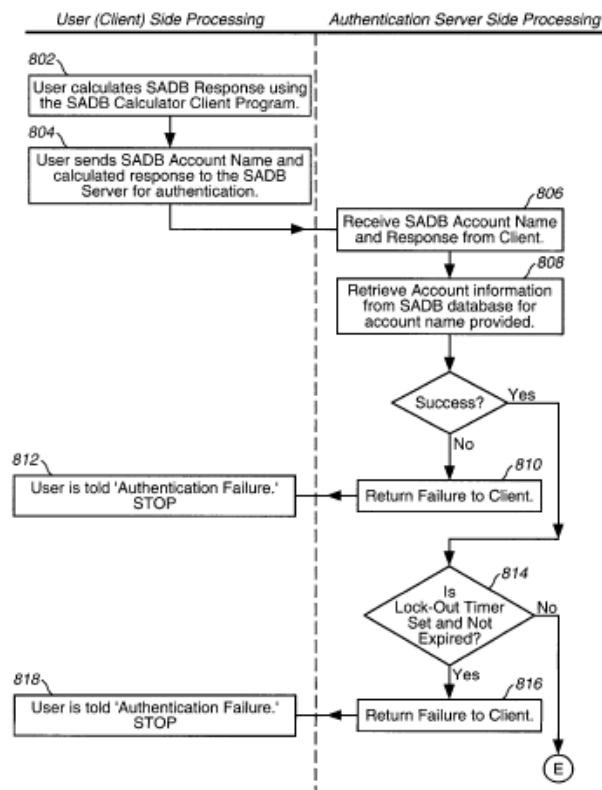


FIG. 8A

If, however, either the flag has not been set or the lockout timer has expired, the authorization process continues. Ex. 1003, ¶150; Ex. 1009, 7:64-8:10, 11:42-49, Figs. 6, 7A, 8A.

A POSITA would have found it obvious to apply this teaching to Lim's account suspension procedures and issue a new challenge after the user's suspension interval has passed to fully take advantage of the benefits of Guthrie's lockout timer. See Section VII.E; Ex. 1003, ¶151. This would ensure that users that fail an Internet access request are suspended only for a specified time period, rather than permanently, which would again allow Lim to accomplish its goal of distinguishing humans from bots more effectively and flexibly. See Section VII.E; Ex. 1003, ¶151. Moreover, Guthrie's disclosure of redirecting to an error page would advantageously advise human users of the error and allow them to understand why their request was not fulfilled. Ex. 1003, ¶151.

In view of the above, Lim alone or in combination with Guthrie render obvious "if said timer is expired, resetting said logged IP address; and proceeding normally with said new request; and if said timer is not expired, dropping or redirecting said TCP connection." Ex. 1003, ¶152.

2. Independent Claim 20

Lim in combination with Guthrie renders Claim 20 obvious. Ex. 1003, ¶153.

[20-PRE] is substantively the same as [1-PRE], and Elements [20-A] through [20-D] are substantively the same as Elements [1-A] through [1-D]. Ex. 1003, ¶154. The only difference between these claims is that while Claim 1 recites a “method...comprising [] steps,” Claim 20 rewrites the method as a “computer process...comprising computer-executable steps.” *Id.*

Lim discloses that its process is computerized and comprises computer-executable steps. Ex. 1004, Fig. 1, 5:5-9:9; Ex. 1003, ¶155.

Thus, Lim in combination with Guthrie discloses Claim 20 for the same reasons discussed above for Claim 1. *See supra* Section VIII.A.1; Ex. 1003, ¶156.

3. Claims 2 and 21

Claim 2 depends from Claim 1 and further requires that “said challenge includes prompting said undefined originator to perform a specific action.” Claim 21 depends from Claim 20 and recites the same additional limitation as that of Claim 2. Ex. 1003, ¶158.

Lim discloses this additional limitation. Ex. 1003, ¶¶157-161.

Lim’s system distinguishes human users from robots by way of a challenge, including challenges which can include multiple graphics or images and text that describes one of those graphics (*i.e.*, a prompt directing the user to select one of the plurality of graphical forms—a specific action). Ex. 1004, Abstract, 2:33-39, 9:53-67, 13:15-28, Claim 1; Ex. 1003, ¶161. The prompt directing a user to answer the

quiz necessarily includes a prompt to perform a specific challenge, *i.e.*, respond to the quiz by selecting the prompted graphic, which is “prompting said undefined originator to perform a specific action.” Ex. 1003, ¶161.

4. Claims 13, 22, 25-26, and 29

Claim 13 depends from Claim 1 and further requires that “said response includes making a choice among a plurality of prompted response options.” Claim 22 depends from Claim 21, and recites this same additional limitation, differing only in terms of non-substantive word choice. Ex. 1003, ¶¶162-164. Claims 25-26 both depend from Claim 20, and also recite this same additional limitation, differing only in terms of non-substantive word choice. *Id.* Claim 29 depends from Claim 2, and recites this same additional limitation. *Id.*

Lim discloses this additional limitation. Ex. 1003, ¶¶162-167.

Lim explains that the prompts for any of its 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, *see also* 13:64-65, 14:42-43; Ex. 1003, ¶166. Lim also 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, ¶166.

Lim, like the ’510 patent, expressly discloses multiple choice questions

selected from an image map and thus renders obvious the quiz “response includes making a choice among a plurality of prompted response options.” Ex. 1003, ¶167.

5. Claims 7, 14, 17, 27, and 30

Claim 7 depends from Claim 2 and further requires that “said response includes an answer to a quiz.” Ex. 1003, ¶¶168-169. Claim 14 depends from Claim 13, and recites this same additional limitation. Ex. 1003, ¶170. Claim 17 depends from Claim 1, and recites this same additional limitation. *Id.* Claim 27 depends from Claim 20, and recites this same additional limitation. *Id.* Claim 30 depends from Claim 29, and recites this same additional limitation. *Id.*

Lim discloses this additional limitation. Ex. 1003, ¶¶168-173.

As above, Lim’s system distinguishes human users from robots by way of a challenge, including challenges that it calls quizzes. Ex. 1004, 2:32-38, *see also* Abstract; Ex. 1003, ¶172. “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).” Ex. 1004, 13:15-18. Lim expressly teaches that the user provides a response to these quizzes. Ex. 1004, 13:33-39 (“The pictures can contain a simple question that any user would be expected to be able to answer.... A separate text box or other data entry device rendered in the web page with the quiz question image could then be used by the user to enter his/her answer.”). Therefore, a POSITA would

understand that Lim discloses quizzes that include a response with an answer to the quiz, as claimed. Ex. 1003, ¶173.

6. Claims 8, 15, 18, and 19

Claim 8 depends from Claim 2 and further requires that “said response is suggested by textual meaning.” Ex. 1003, ¶¶174-175. Claim 15 depends from Claim 13 and recites this same additional limitation. Ex. 1003, ¶176. Claim 18 depends from Claim 17 and recites this same additional limitation. *Id.* Claim 19 depends from Claim 1 and recites this same additional limitation. *Id.*

Lim discloses this additional limitation. Ex. 1003, ¶174-180.

Lim’s quizzes include graphical text prompts, which teach a response suggested by textual meaning. Ex. 1004, 13:29-37, *see also* ,13:64-65 (prompt presented “in graphical text”), 14:42-43 (“[u]sers are asked simple questions using graphical text”); Ex. 1003, ¶178. By presenting the quiz questions “using a display format that cannot be easily recognized or read by a machine or automated process,” Lim thus provides an extra level of security by putting the text of the prompt in an image rather than as plain text. Ex. 1004, 13:29-37, 13:64-65, 14:42-43; *see also* Ex. 1008, 14:8-11 (question “presented in text that is twisted (*i.e.*, displayed in a non-linear fashion) to make optical character recognition (OCR) difficult, while still remaining easily readable to a human”); Ex. 1003, ¶178.

To the extent that the Patent Owner argues this claim requires the prompt to include the answer, Lim expressly discloses quiz questions of the same form as the '510 patent. Ex. 1004, Fig. 4A (prompt is “What color is this yellow box?”); Ex. 1003, ¶179. Another example of a quiz prompt is shown in Fig. 17, which shows graphics depicting several shapes in different colors, and a textual expression suggesting what the response should be: “[c]lick on the yellow triangle.” Ex. 1004, 14:51-53 Ex. 1003, ¶179. Lim discloses additional examples of this concept in its “simple word/object identification/recognition” challenges, which can ask users to “select the correct picture or word matching the object displayed.” Ex. 1004, 13:63-14:5; Ex. 1003, ¶179.

In sum, Lim provides numerous examples of the challenges of the same type as the '510 patent, in which the “response is suggested by textual meaning.” Ex. 1003, ¶180.

7. Claim 28

Claim 28 depends from Claim 20 and further requires “prompting said undefined originator to make a response based upon the knowledge content of said prompt.” Ex. 1003, ¶¶181-182.

Lim discloses this additional limitation. Ex. 1003, ¶¶181-184.

Lim explains that its challenges “may be implemented by using a quiz process that requires user interaction.” Ex. 1004, 2:33-39 (emphasis added); *see*

also, e.g., Abstract, 9:46-67; 13:15-28. Lim explains that the prompts represent simple questions easily answered by a human upon reading the prompt. Ex. 1004, 13:29-37, *see also* 13:64-65 (prompt presented “in graphical text”), 14:42-43 (“[u]sers are asked simple questions using graphical text”); Ex. 1003, ¶184.

Because Lim discloses challenges intended to distinguish humans from robots, just like the ’510 patent, it presents quizzes that prompt the “undefined originator to make a response based upon the knowledge content of said prompt.” Ex. 1003, ¶¶184. That is the fundamental purpose of a quiz question, providing a prompt that provides the information needed (perhaps with additional personal knowledge) to answer the quiz. *See, e.g.*, Ex. 1004, Fig. 4E (assuming the user to know what a “finger” is to respond to the question), Fig. 4C (assuming the user knows geometric shapes to respond to the quiz). Indeed, as explained in Section VIII.A.6, above, for some of Lim’s quizzes, the prompts contain the very answer to quiz itself. Ex. 1004, Fig. 4A. Thus, Lim discloses or renders obvious this limitation. Ex. 1003, ¶184.

B. GROUND 2: Claims 3-6, 9-12, 16, and 23-24 Are Obvious Over Lim In Combination With Guthrie In Further View of Lillibridge

As discussed above, Lim and Guthrie renders obvious independent Claims 1 and 20. *See* Section VIII.A.1 and VIII.A.2; Ex. 1003, ¶185. The additional limitations of Claims 3-6, 9-12, 16, and 23-24 are obvious over Lim and Guthrie in

further view of Lillibridge. Ex. 1003, ¶186.

1. Claims 3, 9, and 23

Claim 3 depends from Claim 2 and further requires that “said prompting is different at each subsequent access of said web site.” Ex. 1003, ¶¶187-188. Claim 9 depends from Claim 1 and recites this same additional limitation. Ex. 1003, ¶189. Claim 23 depends from Claim 20 and recites this same additional limitation, differing only in terms of non-substantive word choice. *Id.*

Lim in combination with Guthrie as in Ground 1 in view of Lillibridge renders this additional limitation obvious. Ex. 1003, ¶190.

Lim explains that a user is given subsequent quiz challenges in the form of a “second prompt” or “next prompt” (*i.e.*, a subsequent access of said web site) after a set time interval has passed after the initial challenge (*i.e.*, the initial request). *See* Ex. 1004, Claim 1 (“determining an amount of time or amount of resources that will be accessible by the human operator before a next prompt is transmitted... and providing a second prompt after expiration of the interval”), 14:58-15:2 (“Users may be quizzed with reduced frequency as they respond accurately and with increasing frequency as they fail to respond accurately. For example, FIG. 5 illustrates a process 500 wherein a new user starts (step 502)” and 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:

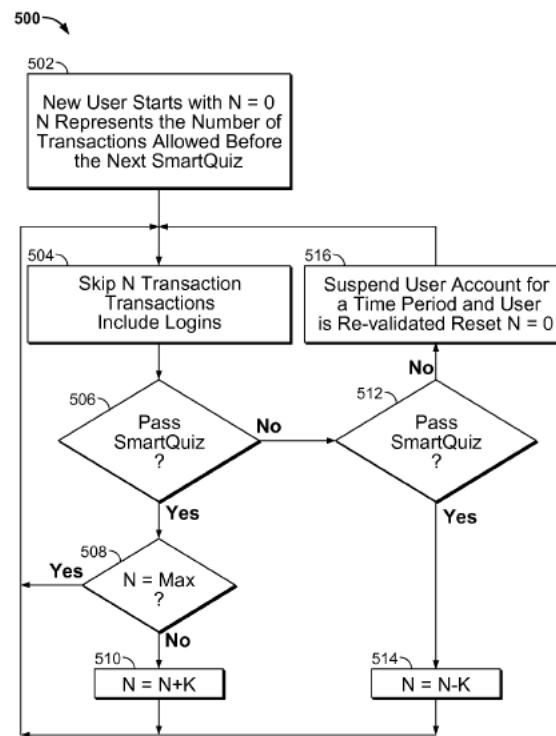


FIG. 5

See also Ex. 1003, ¶191.

In view of these disclosures, 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 subsequent access of said web site. Ex. 1003, ¶192; 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.*, prompting is different at each subsequent access of said web site), as simply repeating the same challenge over and over again would not adequately test the

user. Ex. 1003, ¶193.

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 users. Ex. 1004, 4:7-35, 7:62-8:17, 8:30-35, 9:20-30, Fig. 1; Ex. 1003, ¶194. 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. 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"); Ex. 1003, ¶194. This application of Lim would not work if the user was given the same challenge every time, because a bot would be able to simply repeat the correct answer to that quiz every time and use the website freely, driving up false advertising revenue. Ex. 1003, ¶194.

This concern is reflected in Lim's Fig. 5. 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:

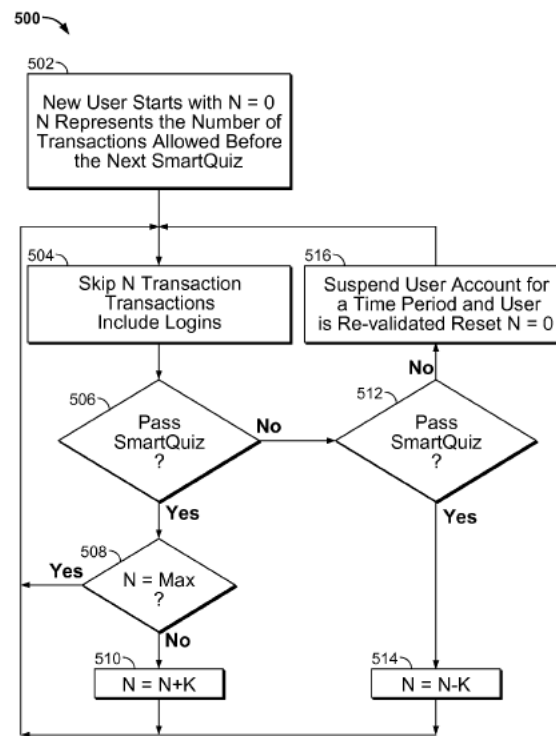


FIG. 5

See also Ex. 1003, ¶195.

Lim's use of the N variable allows one to flexibly set the cadence the site provider believes will balance the user annoyance at having to answer a quiz against the risk the user has turned the system over to a bot. Ex. 1003, ¶196. Moreover, each quiz after N transactions would need to be different to avoid the trivial process of automating a bots answer to the same repeated question. Ex. 1003, ¶196; 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. Ex. 1003, ¶196.

This understanding is confirmed by Lim's statement that its subsequent quizzes are a distinct "next prompt" or "second prompt" and explanation that each of its many challenge embodiments may be used in combination with one another or individually, which suggests a readiness to revise and modify its challenges. Ex. 1003, ¶197; Ex. 1004, Claim 1 ("next prompt" or "second prompt" provided after set interval passes), 3:23-26 ("FIG. 4 illustrates various types of quizzes, any of which may be used in combination with one another or individually"), 3:64-67 ("FIG. 17 illustrates a further example of a quiz, which may be used in combination with other quizzes or individually"), 13:57-59 (example quizzes "may be used in combination with one another or individually"), 14:58-15:2 ("Users may be quizzed with reduced frequency as they respond accurately and with increasing frequency as they fail to respond accurately. For example, FIG. 5 illustrates a process 500 wherein a new user starts (step 502) and is **presented with SmartQuizzes at various intervals** (step 504). As **each quiz** is taken (step 506) a determination is made as to whether the user passed the test. If so (step 508), the interval is adjusted (step 510) until a maximum interval is reached. 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"), Figs. 5, 17 (emphasis added).

A POSITA would have found it particularly obvious to modify the quiz of Lim in view of Lillibridge. Ex. 1003, ¶198.

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. Ex. 1003, ¶199. And the POSITA would have understood that the similar combination of Lim with Guthrie (discussed in Section VII.E as used in Ground 1 above) could be predictably combined with Lillibridge in a similar manner for at least the reasons discussed in Section VII.F above. *Id.*

Lim provides an extensive list of example quiz types that can be used. Ex. 1003, ¶200. This provides a POSITA implementing its system many, varied quizzes and quiz types for the system and supports the obvious notion that many quizzes would be needed. *Id.*

Lillibridge provides a complementary teaching of quizzes that are easily modifiable to satisfy many applications. Ex. 1003, ¶201. For example, 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). This range of applications demonstrates a need for different prompting at each subsequent access of said web site. Ex. 1003, ¶201.

Like Lim's, Lillibridge's challenges are riddles used to test if a user is a human or "electronic agent." *See generally*, Ex. 1008, 3:55-6:16; Ex. 1003, ¶202.

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 and notes that relaxed changing could "present a new riddle less frequently," such as every five requests. Ex. 1008, 8:48-52, *see also* Claim 39 (disclosing "rendering an additional riddle" after a predetermined number of access requests); Ex. 1003, ¶203.

A POSITA would thus understand each of Lillibridge's embodiments to describe generating a random riddle with each request. Ex. 1003, ¶204.

In sum, a POSITA reading Lim would have would have understood that its riddles should change over time, because otherwise its system would not achieve its goal of protecting against bots. Ex. 1003, ¶205. Lillibridge confirms the security benefits of generating a different riddle for each request and provides specific teachings of how to implement new riddles in response to repeated access requests. Ex. 1003, ¶205.

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, ¶206. Legitimate human users would easily adapt to different riddles, while bots would not. Ex. 1003, ¶206. In contrast, bots would be able to take advantage of unchanging riddles, undermining Lim's security goals. Ex. 1003, ¶206.

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, ¶207; 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 4, 10, and 24

Claim 4 depends from Claim 3. Ex. 1003, ¶208. The additional limitation of Claim 4 is the same as that of Claim 13—"said response includes making a choice among a plurality of prompted response options"—which is disclosed by Lim as discussed above in Section VIII.A.4. Ex. 1003, ¶209. Claim 10 depends from Claim 9 and recites this same additional limitation. Claim 24 depends from Claim 23 and recites this same additional limitation, differing only in terms of non-substantive word choice. Ex. 1003, ¶210.

Thus, Lim, alone or in combination with Guthrie, discloses Claims 4, 10, and 24 for the same reasons discussed above for Claim 13. *See supra* Section VIII.A.4; Ex. 1003, ¶211.

3. Claims 5, 6, 11, and 12

Claim 5 depends from Claim 4. Ex. 1003, ¶212. The additional limitation of Claim 5 is the same as that of Claim 7—“said response includes an answer to a quiz”— which is disclosed by Lim as discussed above in Section VIII.A.5. Ex. 1003, ¶213. Claim 6 depends from Claim 3 and recites this same additional limitation. Ex. 1003, ¶214. Claim 11 depends from Claim 10 and recites this same additional limitation. *Id.* Claim 12 depends from Claim 9 and recites this same additional limitation. *Id.* Thus, Lim, alone or in combination with Guthrie, discloses Claims 5, 6, 11, and 12 for the same reasons discussed above for Claim 7. *See supra* Section VIII.A.5; Ex. 1003, ¶215.

4. Claim 16

Claim 16 depends from Claim 9. Ex. 1003, ¶216. The additional limitation of Claim 16 is the same as that of Claim 8. Ex. 1003, ¶217. Thus, Lim discloses Claim 16 for the same reasons discussed above for Claim 8. *See supra* Section VIII.A.6; Ex. 1003, ¶217.

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, ¶218. Further, any attempt by Patent Owner to rely on alleged secondary considerations cannot overcome the showing of obviousness detailed above. *Tokai Corp. v.*

Inter Partes Review

United States Patent No. 7,373,510

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 '510 patent and cancel all Challenged Claims.

Inter Partes Review

United States Patent No. 7,373,510

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. 7,373,510 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 12,822 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. 7,373,510 PURSUANT TO 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 and associated Exhibits 1001-1012 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. 7,373,510

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 /
