

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AT&T SERVICES INC., CELLCO PARTNERSHIP D/B/A VERIZON
WIRELESS, AND NOKIA OF AMERICA CORPORATION,

Petitioners,

v.

RIGHTQUESTION, LLC,
Patent Owner.

U.S. Patent No. 10,674,009
Issue Date: June 2, 2020

Title: VALIDATING AUTOMATIC NUMBER IDENTIFICATION DATA

Inter Partes Review No.: IPR2025-00360

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT 10,674,009
UNDER 35 U.S.C. §§311-319 and 37 C.F.R. §§42.1-.80, 42.100-.107**

Mail Stop “PATENT BOARD”
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450

TABLE OF CONTENTS

Contents

PETITIONER’S EXHIBIT LIST	10
Claim Element Table	12
I. Introduction.....	1
II. Overview.....	1
III. Grounds for Standing.....	3
IV. Reasons for the Requested Relief.....	3
V. Background.....	3
A. Summary of the ’009 Patent.....	3
B. Prosecution History	4
C. Claim Construction	5
D. Priority of the Challenged Claims.....	6
E. Person of Ordinary Skill in the Art (“POSA”).....	6
F. State of the Art	7
1. Authentication Using Third Party/Verification Service Providers	7
2. Authentication Using Device Information and Fingerprinting...8	
VI. Identification of challenges	9
A. Challenged Claims	9
B. Statutory Grounds for Challenges	9
1. Ground 1	9
VII. Identification of How the Challenged Claims Are Unpatentable	10

A.	Ground 1: Claims 1-23 are Obvious over Miller	10
1.	Miller Presents Compelling Evidence Of Unpatentability	10
2.	Detailed Application of Miller.....	19
a.	Claim 1.....	19
i.	A system, comprising:.....	19
ii.	a verification service provider, configured to, using one or more processors:.....	19
iii.	enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;	20
iv.	store, at the verification service provider, the device fingerprint associated with the first device;	20
v.	obtain, at the verification service provider, information transmitted by a second device associated with a communications connection;	28
vi.	perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and	37

vii.	based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.	45
b.	Claim 2:	50
c.	Claim 3.....	53
d.	Claim 4.....	54
e.	Claim 5.....	55
f.	Claim 6.....	55
g.	Claim 7.....	59
h.	Claim 8.....	62
i.	Claim 9.....	63
j.	Claim 10.....	65
i.	A method, comprising:.....	66
ii.	enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;	66
iii.	storing, at the verification service provider, the device fingerprint associated with the first device;	66
iv.	obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;.....	67

v.	performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and;	67
vi.	based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.	67
k.	Claim 11.....	68
l.	Claim 12.....	68
m.	Claim 13.....	69
n.	Claim 14.....	69
o.	Claim 15.....	69
p.	Claim 16.....	70
q.	Claim 17.....	70
i.	A computer program product embodied in a tangible and non-transitory computer readable storage medium and comprising computer instructions for:	71
ii.	enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of	

	configuration information associated with the first device;	71
iii.	storing, at the verification service provider, the device fingerprint associated with the first device;	72
iv.	obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;.....	72
v.	performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated baed at least in part on the set of configuration information associated with the enrolled first device; and;	72
vi.	based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.	73
r.	Claim 18.....	73
s.	Claim 19.....	73
t.	Claim 20.....	74
u.	Claim 21.....	74
v.	Claim 22.....	75
w.	Claim 23.....	75
VIII.	The Board Should Not exercise its discretion to deny institution Under <i>Fintiv</i>	76

IX.	Mandatory Notices under 37 C.F.R. §42.8.....	79
A.	Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1).....	79
B.	Related Matters Under 37 C.F.R. § 42.8(b)(2)	80
C.	Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)	81
D.	Service Information Under 37 C.F.R. § 42.8(b)(4).....	82
X.	CONCLUSION.....	82
	CERTIFICATION OF SERVICE ON PATENT OWNER.....	83
	CERTIFICATE OF COMPLIANCE.....	85

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Apple Inc. v. Fintiv, Inc.</i>	77
<i>Dish Network v. Broadband iTV</i> IPR2020-01280, Paper 17 (PTAB Feb. 4, 2021)	79
<i>HP Inc. v. Slingshot Printing LLC</i> IPR2020-01084, Paper 13 (Jan. 14, 2021)	80
<i>PEAG LLC v. Varta Microbattery GMBH</i> IPR2020-01214, Paper 8 (Jan. 6, 2021)	79
<i>RightQuestion, LLC v. AT&T Inc. et al</i> 2:24-cv-00094 (E.D. Tex.)	81
<i>RightQuestion, LLC v. Cellco, Verizon Business Network Services</i> <i>LLC et al.</i> No. 2:24-cv-00091 (E.D. Tex.)	81
<i>Sand Revolution II LLC v. Continental Intermodal Group – Trucking</i> <i>LLC</i> IPR2019-01393, Paper 24 (June 16, 2020)	78
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> IPR2020-01019, Paper 12 (Dec. 1, 2020)	78
STATUTES	
35 U.S.C. § 102(a)(1) (pre-AIA)	9
35 U.S.C. § 311	1
OTHER AUTHORITIES	
37 C.F.R. § 42.1	1
37 C.F.R. §42.104(a)	3
37 C.F.R. §42.106(a)	3

37 C.F.R. § 42.108	1
<u>https://txed.uscourts.gov/?q=model-order-focusing-patent-claims-and-prior-art-reduce-costs</u>	80

PETITIONER’S EXHIBIT LIST

<i>Exhibit #</i>	<i>Description</i>
1001	U.S. Patent No. 10,674,009 (“’009 Patent”)
1002	File History for U.S. Patent No. 10,974,009
1003	Expert Declaration of Patrick McDaniel
1004	Intentionally Omitted
1005	Intentionally Omitted
1006	Intentionally Omitted
1007	AT&T Amended Infringement Contentions Exhibit A (’009 Patent), <i>RightQuestion, LLC v. AT&T Corp., et al.</i> , No. 2:24-cv-00094-JRG (E.D. Tex.) Served: October 7, 2024.
1008	Second Amended Docket Control Order in <i>RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.</i> , No. 2:24-cv-00091 (E.D. Tex., October 20, 2024) (Lead Case)
1009	Dave Otway and Owen Rees. 1987. Efficient and timely mutual authentication. SIGOPS Oper. Syst. Rev. 21, 1 (Jan. 1987), 8–10. https://doi.org/10.1145/24592.24594
1010	Simpson, E., Schaumont, P. (2006). Offline Hardware/Software Authentication for Reconfigurable Platforms. In: Goubin, L., Matsui, M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. CHES 2006. Lecture Notes in Computer Science, vol 4249. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11894063_25 (“Simpson”)
1011	Loh Chin Choong Desmond, Cho Chia Yuan, Tan Chung Pheng, and Ri Seng Lee. 2008. Identifying unique devices through wireless fingerprinting. In Proceedings of the first ACM conference on Wireless network security (WiSec '08). Association for Computing Machinery, New York, NY, USA, 46–55. https://doi.org/10.1145/1352533.1352542
1012	Ke Gao, C. Corbett and R. Beyah, "A passive approach to wireless device fingerprinting," <i>2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)</i> , Chicago, IL, 2010, pp. 383-392, doi: 10.1109/DSN.2010.5544294.

<i>Exhibit #</i>	<i>Description</i>
1013	Martins, Rui & Augusto, Alexandre & Correia, Manuel Eduardo. (2013). A Potpourri of Authentication mechanisms - The mobile device way. May 2013, Conference: 8 ^a Conferencia Ibérica de Sistemas y Tecnologías de Informaci3n (CISTI 2013)
1014	Abu-Hakima, Suhayya, Mansour Toloo and Tony White. “A Multi-Agent Systems Approach for Fraud Detection in Personal Communication Systems.” (2002).
1015	Hossain, A.K.M. Mahtab & Jin, Yunye & Soh, Wee-Seng & Van, Hien. (2013). SSD: A Robust RF Location Fingerprint Addressing Mobile Devices' Heterogeneity. Mobile Computing, IEEE Transactions on. 12. 65-77. 10.1109/TMC.2011.243.
1016	AT&T Infringement Contentions Cover Pleading, <i>RightQuestion, LLC v. AT&T Corp., et al.</i> , No. 2:24-cv-00094-JRG (E.D. Tex.) Served: May 14, 2024.
1017	Boris Danev (2011) Physical-Layer Identification of Wireless Devices [Doctoral dissertation, ETH Zurich]. ETH Zurich Library Collection. https://www.research-collection.ethz.ch/handle/20.500.11850/72822
1018	Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. ACM Comput. Surv. 45, 1, Article 6 (November 2012). https://doi.org/10.1145/2379776.2379782
1019	Plaintiff’s Preliminary Claim Construction (E.D. Tex. Local Patent Rule 4-2) in <i>RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.</i> , No. 2:24-cv-00091) (Lead Case) Served: January 8, 2025
1020	Preliminary Claim Construction (E.D. Tex. Local Patent Rule 4-3) in <i>RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.</i> , No. 2:24-cv-00091) (Lead Case) Served: January 27, 2025
1021	U.S. Patent Publication No. 2012/0201381 (“Miller”)
1022	U.S. Patent No. 11,005,989 (“989 Patent”)

Claim Element Table

Element	Claim Language
1.i	1. A system, comprising:
1.ii	a verification service provider, configured to, using one or more processors:
1.iii	enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;
1.iv	store, at the verification service provider, the device fingerprint associated with the first device;
1.v	obtain, at the verification service provider, information transmitted by a second device associated with a communications connection;
1.vi	perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and
1.vii	based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.
2	2. The system of claim 1, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.
3	3. The system of claim 1, wherein based at least in part on the security determination, the verification service provider is further configured

	to convey an assurance to a recipient associated with the communications connection.
4	4. The system of claim 1, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.
5	5. The system of claim 1, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.
6	6. The system of claim 1, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.
7	7. The system of claim 1, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.
8	8. The system of claim 1, wherein the set of configuration information comprises at least one of a set of device settings, a set of installed applications, system version information, application software version information, and a contact list associated with the first device.
9	9. The system of claim 1, wherein the verification service provider is further configured to re-enroll the first device in response to a determination of a change in the device fingerprint.
10.i	10. A method, comprising:
10.ii	enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;
10.iii	storing, at the verification service provider, the device fingerprint associated with the first device;

10.iv	obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;
10.v	performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and
10.vi	based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.
11	11. The method of claim 10, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.
12	12. The method of claim 10, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.
13	13. The method of claim 10, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.
14	14. The method of claim 10, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.
15	15. The method of claim 10, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.
16	16. The method of claim 10, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card

	information validation, and a check of at least one of a name, an address, and a phone number.
17.i	17. A computer program product embodied in a tangible and non-transitory computer readable storage medium and comprising computer instructions for:
17.ii	enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;
17.iii	storing, at the verification service provider, the device fingerprint associated with the first device;
17.iv	obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;
17.v	performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and
17.vi	based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.
18	18. The computer program product of claim 17, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.
19	19. The computer program product of claim 17, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.

20	20. The computer program product of claim 17, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.
21	21. The computer program product of claim 17, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.
22	22. The computer program product of claim 17, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.
23	23. The computer program product of claim 17, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.

I. INTRODUCTION

AT&T Services Inc., Cellco Partnership D/B/A Verizon Wireless, and Nokia of America Corporation, (collectively, “Petitioners” or “Petitioner”) hereby petition for an *inter partes* review (“IPR”) of Claims 1-23 (the “Challenged Claims”) of U.S. Patent No. 10,674,009 (the “’009 Patent”). *See* 35 U.S.C. § 311, 37 C.F.R. § 42.1. Petitioner respectfully requests that the Board institute an *inter partes* review of the ’009 Patent, pursuant to 37 C.F.R. § 42.108, because this Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail.

II. OVERVIEW

The ’009 Patent purports to provide a novel technique for verifying a device initiating a communication. The Challenged Claims are directed at storing device information and other data with a verifying entity, so that when a communication occurs, information about the originating device can be verified against previously stored device information. This device information comparison is then used to perform a security determination for treatment of the communication. Ex-1003, ¶¶25-26.

As detailed below, the prior art herein teaches the same architecture and functionality that the ’009 patent (later) disclosed and claimed. Miller discloses a system in which unique device information (referenced as “computer fingerprint” or

“computer minutia”) is registered / enrolled with a trusted verification entity which stores this device information. During subsequent communications, the trusted entity compares the stored (known) device information against information received from a device attempting communication. Depending on this comparison, Miller’s system will deny the communication, allow the communication or seek further information from the device to use for verification. Ex-1003, ¶27.

As detailed in Section V.B, the ’009 claims were allowed on the basis of citations to a “device fingerprint.” However, Miller describes (and uses) the same sort of device / computer fingerprint information as taught in the ’009 patent:

Miller	’009 Patent
A “computer fingerprint typically uses computer minutiae” and Miller’s “computer minutia” are sets of “device manufacturer, model number, serial number, ... the name of the firmware vendor, version number, revision number, revision date, ... operating system. application name, ... software release number, memory reads, software cataloging, clock and other counters, and date” and “contact phone numbers.” Ex-1021, [0011], [0052].	A “device “fingerprint” created from a combination of device settings, installed applications, system or application software versions, or contact list stored on the phone.” Ex-1001, 9:31-34.

Ex-1003, ¶28.

The prior art below presents compelling and overwhelming evidence of invalidity. Petitioners respectfully request that the Board institute IPR and cancel the Challenged Claims. Ex-1003, ¶29.

III. GROUNDS FOR STANDING

Petitioners certify that the '009 Patent is available for IPR and Petitioners are not barred or estopped from requesting this review. 37 C.F.R. §42.104(a). This Petition is being filed less than one year after the date on which Petitioners (or a privy of Petitioners) were served with a Complaint alleging infringement of the '009 Patent. This Petition is filed under 37 C.F.R. §42.106(a).

IV. REASONS FOR THE REQUESTED RELIEF

As explained in this Petition and the Declaration of Petitioners' Expert, Prof. Patrick McDaniel (Ex-1003), the systems, methods, and computer program products claimed in the '009 Patent were obvious in view of the prior art to a POSA at the time of the invention.

V. BACKGROUND

A. Summary of the '009 Patent

The '009 Patent describes “techniques for ascertaining the identity of a device initiating communications” to detect “potential attempts at spoofing of caller ID or automatic caller identification (ANI) data.” Ex-1001, 2:41-57; Ex-1003, ¶30.

To combat spoofing, the '009 Patent describes using a verification service that enrolls a user's device identification information. Ex-1001, 9:17-54. In various embodiments, the verification service stores information associated with a user's device based on unique hardware and/or software details. *Id.* When either party involved in a communication needs to verify the identity of the other party, a request can be made to the verification service, which retrieves the enrolled device's information. Ex-1001, 2:59-3:3, 4:38-46, 14:23-56, 22:16-29. The verification service can compare device identification and other information against stored information. Ex-1001, 9:17-54. Based on the comparison of device information, a security determination can be made to include "blocking access, requesting additional authentication factors, permitting access, etc." *Id.* 9:53-54; Ex-1003, ¶31.

B. Prosecution History

The Challenged Claims are the result of a single amendment to the original claims, made in response to one non-final office action during prosecution. During prosecution, the Examiner rejected all claims as being anticipated by U.S. Patent No. 9,060,057 to Danis. Ex-1002, 153-162. Following a telephonic interview, the Applicant amended independent claims 1, 8, and 15 to add that "fingerprint" is stored and used in the security determination.

1. (Currently amended) A system, comprising:
 - a verification service provider, configured to, using one or more processors:
 - enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with ~~device information comprising at least one of a software identifier, an embedded hardware identifier, and a device fingerprint that, wherein the device fingerprint is~~ generated based at least in part on a set of configuration information associated with the first device;
 - store, at the verification service provider, the device fingerprint information associated with the first device;
 - obtain, at the verification service provider, information transmitted by a second device associated with a communications connection;
 - perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device ~~device information associated with the enrolled first device~~; and
 - based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.

Ex-1002, 195-201.¹

The Challenged Claims were allowed based on this amendment.

C. Claim Construction

Petitioner proposes that each claim term be given its plain and ordinary meaning as would be understood in the context of the specification, and that no

¹ The amendment to independent claim 1 (system) is similar to the amendments to claims 10 (method) and 17 (computer program).

specific construction of any claim term is required in this proceeding because at least one ground identified in this Petition meets the claims under any reasonable construction.²

In the co-pending litigation, the parties have exchanged proposed constructions. Ex-1019, Ex-1020. The prior art herein meets the claim limitations below under all of the proposed constructions.

D. Priority of the Challenged Claims

The '009 Patent was filed on November 5, 2018. EX-1001, Cover. Petitioners herein use the November 7, 2013 priority date alleged by the Patent Owner (“Priority Date”). Ex. 1016, VI; Ex-1003, ¶34.

E. Person of Ordinary Skill in the Art (“POSA”)

A POSA for the '009 Patent would have had at least a bachelor’s degree in computer science, electrical engineering, or a related technical field, and at least two years of professional experience, or an equivalent advanced education, in the field of security of cellular / telephony networks and mobile systems. Additional work experience in relevant industries could compensate for less education or education in a different field, and vice versa. EX-1003, ¶¶35-38.

² This interpretation is only applicable to this *inter partes* review. Petitioners expressly reserve the right to present an interpretation of a claim term in other proceedings, which is different from that presented in this Petition.

F. State of the Art

1. Authentication Using Third Party/Verification Service

Providers

Using third party authentication/verification services to ascertain a mobile device's identity was known, at least as early as 2001. Specifically, a fundamental concept in wireless networks is "roaming" (maintaining wireless connectivity outside of a subscriber's coverage area). A roaming subscriber must register with a database before calling on the visiting network. *Id.* The registration information is then transferred from the visitor's network to the subscriber's network where the home location register ("HLR") database resides. *Id.* The HLR is a database of user identity information related to the mobile device. The visiting location register ("VLR") is a database of information for devices roaming. When a call is made, an authentication center matches device information stored in the HLR database with the information received from the VLR, to the mobile device is authenticated for access on the network. Ex-1003, ¶¶40-42.

More broadly, enrolling device-specific information with a verification service provider for authentication was well-known at the time of the invention. Ex-1010, 313-317; Ex-1003, ¶¶43-44.

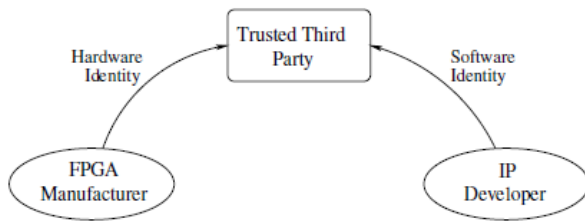


Fig. 3. Enrollment Phase

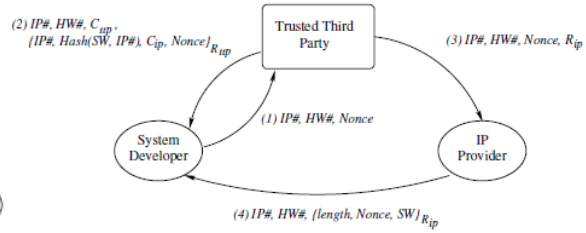


Fig. 4. Distribution Phase

Ex-1010, Figs. 3-4

2. Authentication Using Device Information and Fingerprinting

It has long been known that fingerprints can be collected from devices. *See e.g.*, Ex-1012 (“Fingerprinting networked devices has been around for many years. The general idea is to extract leaked information about the device's software, operating system, or hardware components.”); Ex-1017, Abstract, Chapter 3 (Device Identification Background), Figure 3.1; Ex-1018, 6:2-6:3. Device identity spoofing has also long been prevalent, as bad actors can “easily clone a Mobile Identification Number (MIN) and its associated Equipment Serial Number (ESN)” using “mobile communications scanners.” Ex-1014; Ex-1003, ¶¶45-46.

The device fingerprint could be based on a device signal strength (such as an RF fingerprint associated with the device or class of device). Using device fingerprinting (either alone or in combination with other authentication techniques, including public and private key encryption) goes back decades—by 1997, academics were discussing how cellular devices could be fingerprinted to stop

identity thieves. Device fingerprinting in wireless communications systems was well known prior to the '009 Patent Priority Date. *See e.g.*, Ex-1011(fingerprinting using hardware and software device information); Ex-1015(fingerprinting a mobile device's geolocation); Ex-1017, Abstract, Chapter 3 (Device Identification Background), Figure 3.1; Ex-1018, 6:2-6:3. Ex-1003, ¶¶47-48.

VI. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 1-23 of the '009 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

Challenges are set forth in detail below and summarized as follows:

Ground	Claim(s)	Basis	Reference
1	1-23	§103	Miller

1. Ground 1

Miller (Ex-1021) was filed February 3, 2012, published August 9, 2012, and is prior art under at least 35 U.S.C. AIA 102(a)(1). Miller was not cited or applied by the Examiner during prosecution of the '009 Patent or its parent application.

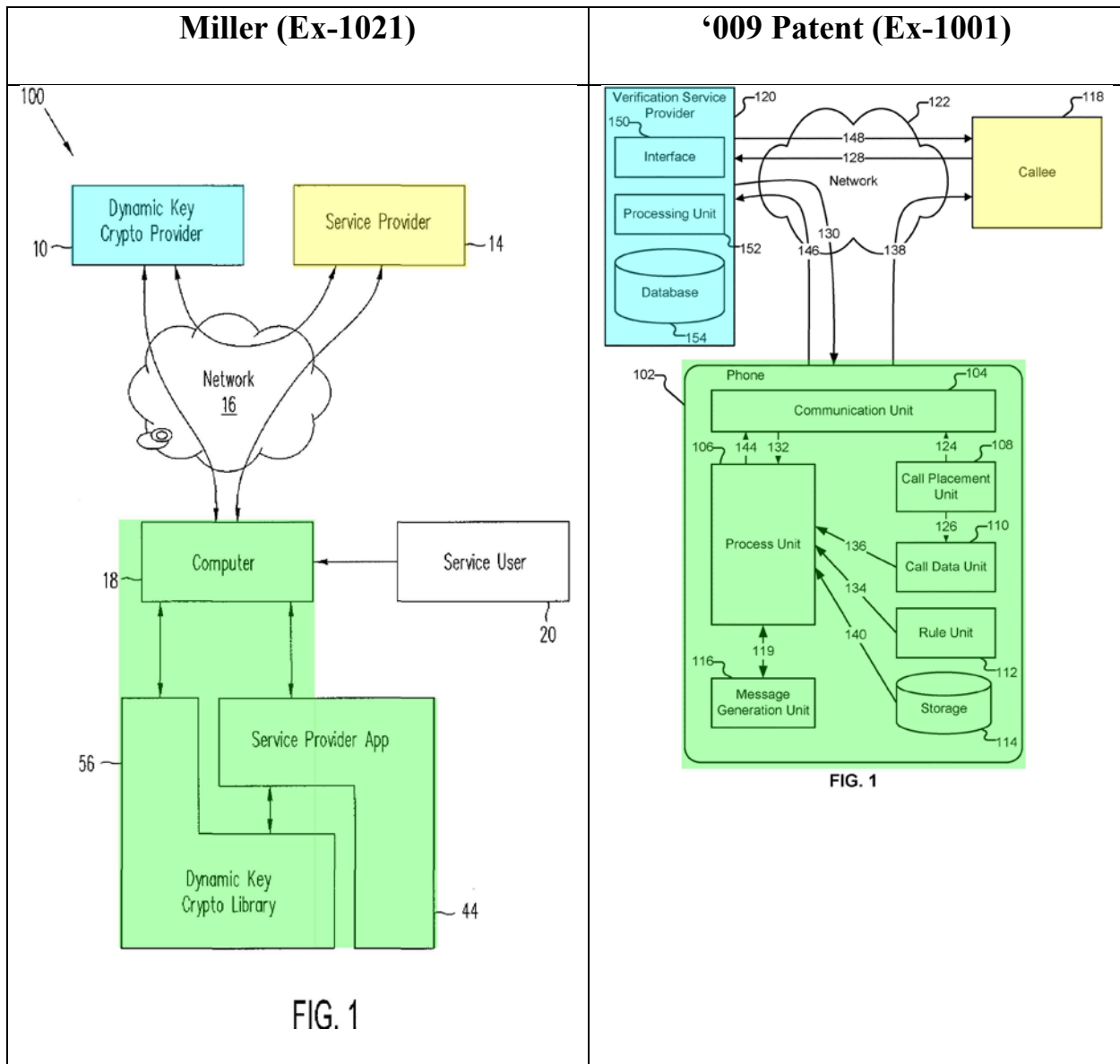
VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-23 are Obvious over Miller

1. Miller Presents Compelling Evidence Of Unpatentability

Miller teaches a system for authorizing / verifying the identity of a particular device involved in a communication. For such verification, Miller “uniquely identif[ies] the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device.” Ex-1021, Abstract; Ex-1003, ¶51.

The '009 patent adopted (and claimed) an architecture and processes largely matching Miller's disclosure. For example, Figures 1 from each of Miller and the '009 patent shows the matching relevant components in the communication.



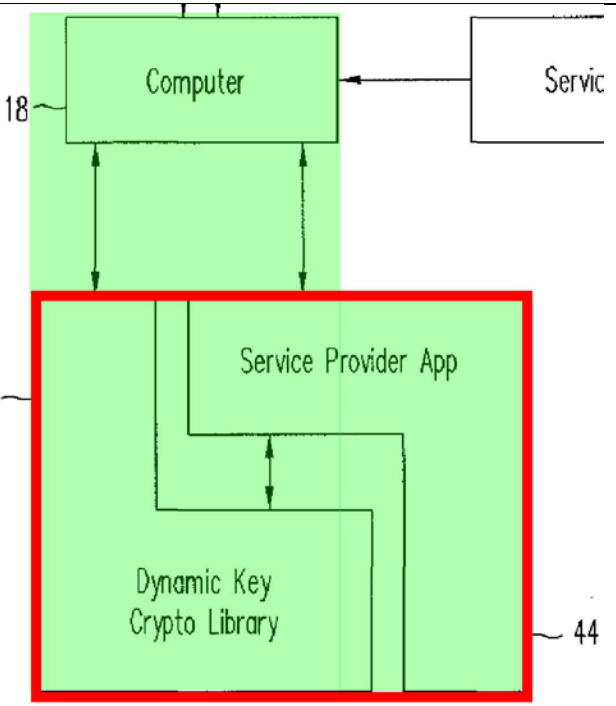
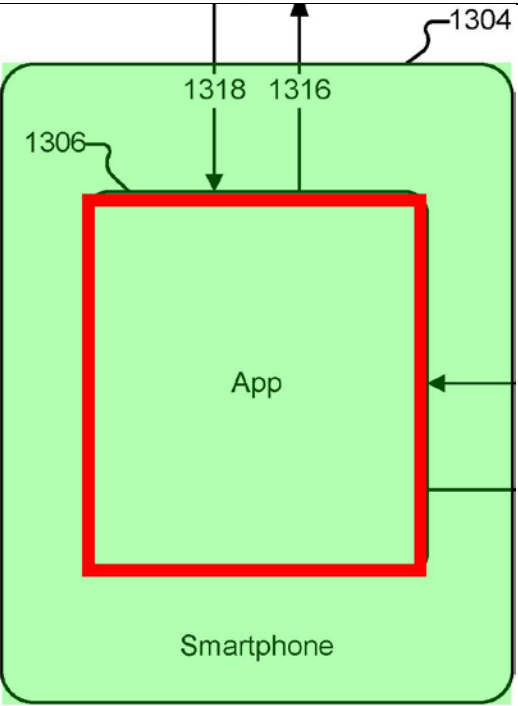
Miller and the '009 patent each teach communication between a first device (green) and a second device (yellow) for which the “first device” is authorized / verified by a verification provider (blue) which Miller calls a “dynamic key crypto provider” (herein, “DKCP”) and the '009 patent calls a “verification service provider” (herein, “VSP”). Ex-1003, ¶52.

Miller and the '009 patent describe the same types of “devices” in the communication.

Miller devices	'009 Patent devices
“e.g., a mobile phone, computer system, smart phones, laptops, tablets, ... or any other communication capable electronic computer.” Ex-1021, [0048].	“a smartphone, tablet, PC, phablet, or wearable computer.” Ex-1001, 12:26-31.

Ex-1003, ¶53.

Miller and the '009 patent both teach that an “app” may be used on the device to facilitate verification.

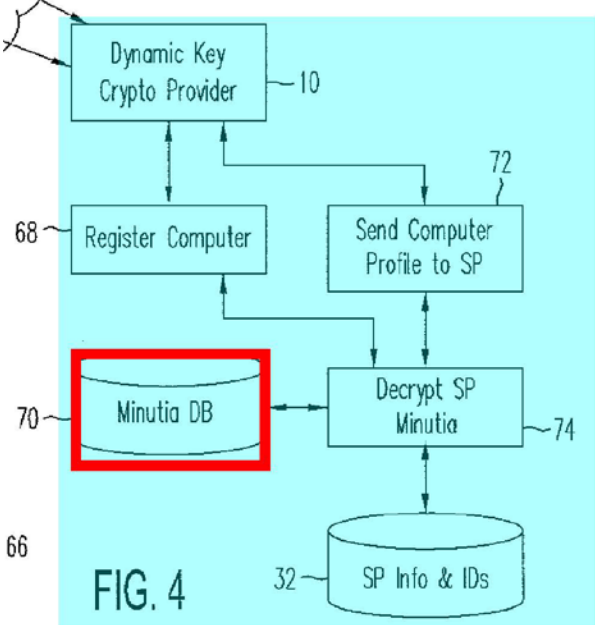
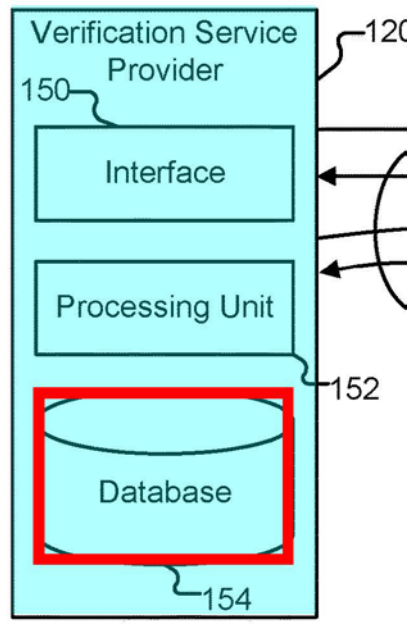
Miller (Ex-1021, Fig. 1)	'009 Patent (Ex-1001, Fig. 13)
 The diagram shows a Computer (18) at the top, connected to a Service Provider App and a Dynamic Key Crypto Library (44) below it. The Service Provider App and Dynamic Key Crypto Library are enclosed in a red rectangular border. A Service box is also connected to the Computer.	 The diagram shows a Smartphone (1304) containing an App (1306). The App is highlighted with a red rectangular border. Arrows labeled 1318 and 1316 indicate communication between the App and the Smartphone.
[0048] (“computer 18 (also referred to as “electronic device”, “user device”, or simply “device”) may operate by executing an operating system (OS) that may enable execution on computer 18 of a dynamic key crypto library 56 and a service provider app 44”)	5:60-63 (“portions of the verification process are performed as part of an application (also referred to herein as an “app”) that is installed on an end-user phone device.”), 7:3-25, 22:18-29.

Ex-1003, ¶54.

Miller's DKCP and the '009 patent VSP are both implemented as computer servers using the typical server hardware such as processors, memories and software. Ex-1021, [0177-0179]; Ex-1001, 4:5-22; Ex-1003, ¶55.

Miller teaches the same functional steps that the '009 patent later regurgitated and attempted to claim. First, both Miller and the '009 patent register devices with the DKCP/VSP using unique device identifiers – which Miller calls “computer minutia” or “computer fingerprints” and the '009 calls a “device fingerprint.” See Section II, *supra*. Ex-1003, ¶56.

Second, both Miller's DKCP and the '009 patent VSP store the enrolled device information (fingerprint/minutia) in databases for later usage.

Miller (Ex-1021, Fig. 4)	'009 Patent (Ex-1001, Fig. 1)
 FIG. 4	
[0092] (“The minutia DB 70 can store the type (or category) of minutia, its value and the service identifier for later processing”)	3:65-67 (“database 154 is a data store configured to store information associated with performing verification.”)

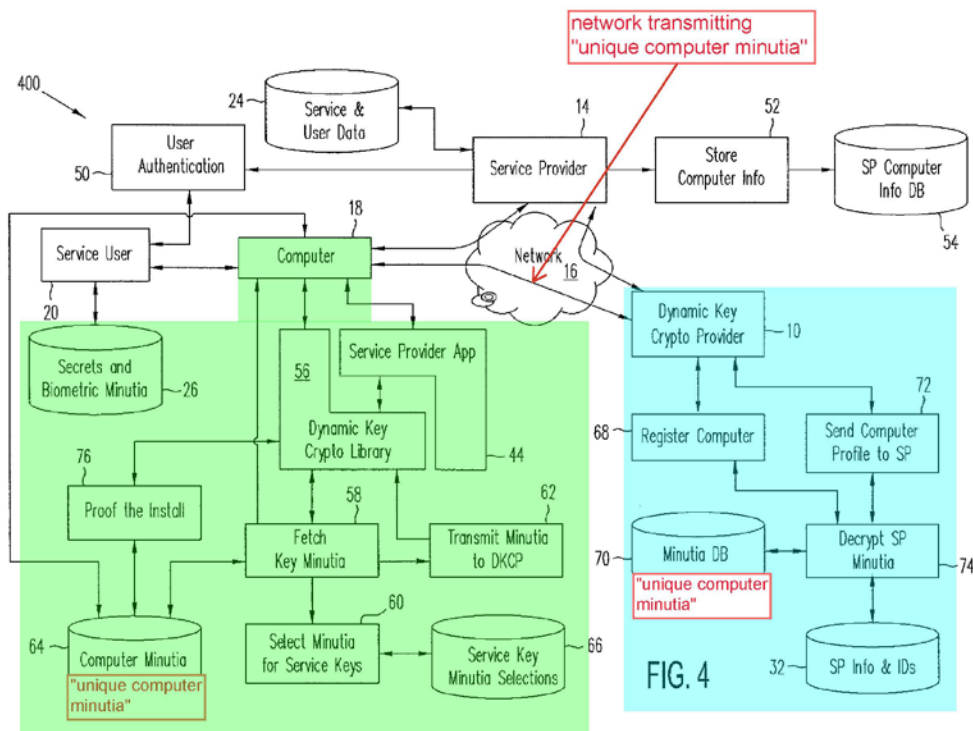
Ex-1003, ¶57.

Third, both Miller’s DKCP and the ’009 patent VSP receive a device information (fingerprint / minutia) from the device during the authentication process.

Miller

(Ex-1021,

Fig. 4)

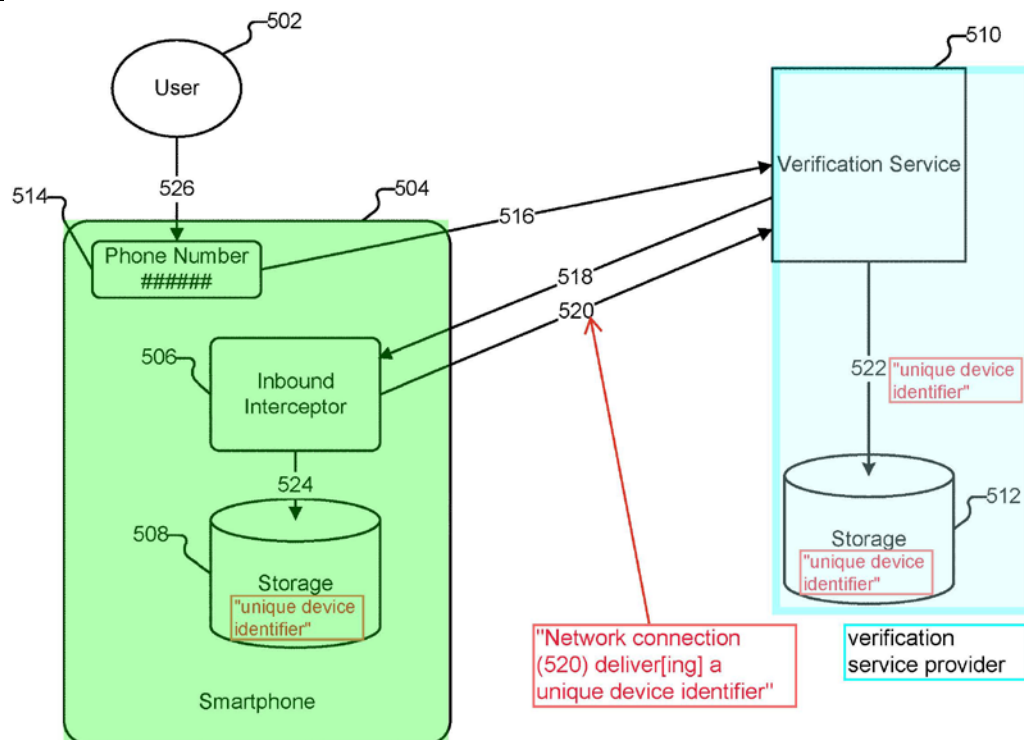


'009

Patent

(Ex-1001,

Fig. 5)



Ex-1003, ¶58.

Fourth, both Miller’s DKCP and the ’009 patent VSP compare the registered minutia / enrolled fingerprint against the minutia / fingerprint received from a device seeking authentication.

Miller (Ex-1021)	’009 Patent (Ex-1001)
Ex-1021, [0066] (“comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match”);	Ex-1001, 9:24-26 (“the verification service evaluates the device information and unique identifier to determine a match against previous usage of the device that is recorded and stored at the verification service”).

Ex-1003, ¶59.

Fifth, both Miller’s DKCP and the ’009 patent VSP teach calculating a “score” based upon the device’s information (and enrollment information) and various other factors to help determine authenticity.

Miller (Ex-1021)	'009 Patent (Ex-1001)
Ex-1021, [0105] (“The compute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130,”);	Ex-1001, 9:39-45 (“the verification score is created using a variety of approaches that include one or more of combining the available factors to create a score ...”)

Ex-1003, ¶60.

Sixth, both Miller’s DKCP and the ’009 patent VSP select actions, such as blocking (denying) communication, allowing communication, or seeking further information, such as PIN’s or passwords from the users.

Miller (Ex-1021)	'009 Patent (Ex-1001)
The verification process may result in “denying the service request” [0118]; or “the allow user action 182 may be performed” [0119] or perform a new request / “challenge” for further verification minutia [0112-0116].	Ex-1001, 9:51-54 (“The decision system then selects from a range of appropriate responses, which include at least one of blocking access, requesting additional authentication factors, permitting access, etc.”).

Simply put, Miller discloses the same architecture and functionality that the '009 patent subsequently disclosed and claimed. Ex-1003, ¶61.

2. Detailed Application of Miller

Claim 1 teaches two aspects of the verification process. First, claim 1 recites an “enroll” process in which the data used to authenticate a device (“*device fingerprint*”) is provided to the verification service provider which stores that “device fingerprint.” Second, claim 1 recites the usage of the “device fingerprint” information to verify that a device involved in a communication corresponds to the enrolled / registered device. Ex-1003, ¶62

Miller details both aspects – using substantially similar terminology that the (later) '009 patent adopted for its specification. Ex-1003, ¶63.

a. Claim 1

i. A system, comprising:

If the preamble is limiting, as detailed below, Miller discloses the claimed system in Figs. 1-9. Ex-1021, Figs. 1-9. Ex-1003, ¶¶64.

ii. a verification service provider, configured to, using one or more processors:

Miller’s “dynamic key crypto provider” (“DKCP”) (*verification service provider*) uses “processors” to execute software code to perform its functions

detailed below articulated for the claimed verification service provider to verify / authenticate a device. Ex-1021, [0049] (DKCP “may provide a secured processing environment...”) [0015-0016], [0178-0180], [0183-0185], claims 24-34 (“server” and “processor”). Ex-1003, ¶65.

- iii. enroll a first device with the verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;
- iv. store, at the verification service provider, the device fingerprint associated with the first device;

These elements describe enrolling or registering a device using a “device fingerprint” so that the “device fingerprint” can be used in a later element for verification of the device. Ex-1001, 17:33-18:35, 11:55-58 (“caller device is registered a single time with a verification service and is then able to use the verification service with many called parties”), Figs 3A-3B. Miller’s DKCP (*verification service provider*) registers (*enrolls*) a “computer 18” (*first device*) and

stores unique device identifiers (*device fingerprint*) for later verification of that device. Ex-1021, Fig. 4, [0020]; [0085] (“FIG. 4 shows a system for registering a computer 18 with a dynamic key crypto provider 10...”). Ex-1003, ¶66.

Miller creates a unique device identifier based on a set / combination of “computer minutia,” (*device fingerprint that is generated based at least in part on a set of configuration information associated with the first device*) to uniquely identify individual computers 18 (*first device*).

[S]ystem 200 may collect and catalog a number of minutiae values of computer 18 and service user 20 that may be useful for identifying the computer 18 and service user 20 in the sense that computer minutia 64 and secrets and biometric minutia 26 can be used by the dynamic key crypto provider 10 to form dynamic keys unique to each and every distinct computer 18 and service user 20. In other words, each distinct computer 18 may have a method for using unique computer minutia 64 and secrets and biometric minutia 26 in system 200 that corresponds to that distinct computer 18 and service user 20, and each uniquely identified computer 18 corresponds to one and only one distinct computer 18 and each uniquely identified service user 20 may correspond to one and only one distinct service user 20. The unique identification of a computer 18 may be processed by system 100, for example, by a service provider 14 or by the dynamic key crypto provider 10 ...

Ex-1021, [0050]; Ex-1003, ¶67.

Miller uses the device configuration information as the '009 patent identifies as the basis for a “fingerprint.” For example, the '009 states:

a device “fingerprint” created from a combination of device settings, installed applications, system or application software versions, or contact list stored on the phone.

Ex-1001, 9:31-33; *see also* Ex-1001, claim 9; Ex-1003, ¶68.

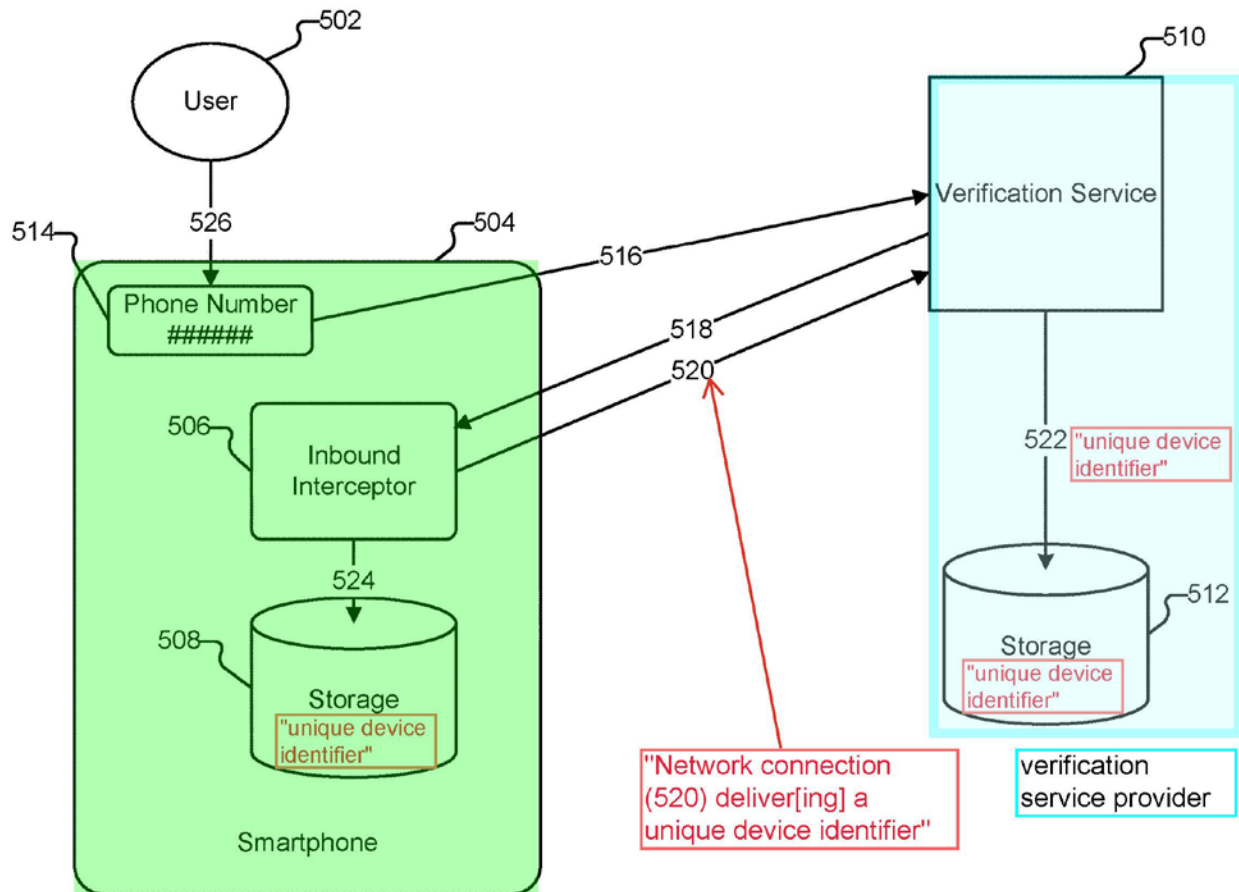
Miller’s “computer minutia” includes different permutations of “hardware,” “firmware” and “software” minutia. Ex-1021, [0057-0061]; Figs. 2A-2B. Miller’s computer minutia discloses the same type of information specified for the '009 fingerprint. In Miller, “examples of firmware and software minutia may include which firmware and software codes are installed on the computing device and characteristics such as what particular version or release date of firmware or software are installed on the computing device” – matching the '009 patent’s identification of a fingerprint as including “installed applications, system or application software versions.” Ex-1021, [0031]. “Firmware minutiae may include ... version number, revision number, ... and operating system” and different forms of “hardware” and “firmware” minutia. Ex-1021, [0052], [0055]. Miller’s computer minutia includes “contacts” and “contact phone numbers” (*contact list*). Ex-1021, [0056]. Miller identifies device settings and device-specific identifiers used for the computer minutia. Ex-1021, [0031] (“make and model of the computing device ... an

international mobile equipment identification (IMEI) number of the computing device, or a circuit manufacturer's ID number”). Ex-1003, ¶69.

Miller also expressly teaches the claimed *device fingerprint* as a “hash” of combination of different minutia. “Computer and computer identification has been attempted by calculating a hash of the minutia found on a computer to uniquely identify the computer, often referred to as a computer fingerprint.” Ex-1021, [0011]. As detailed for elements 1.v and 1.vi *infra*, Miller teaches a “hash” with computer minutia being used to authenticate devices. Ex-1021, [0039], [0051], [0094], [0132-0133], [0142-0143]. Ex-1003, ¶70.

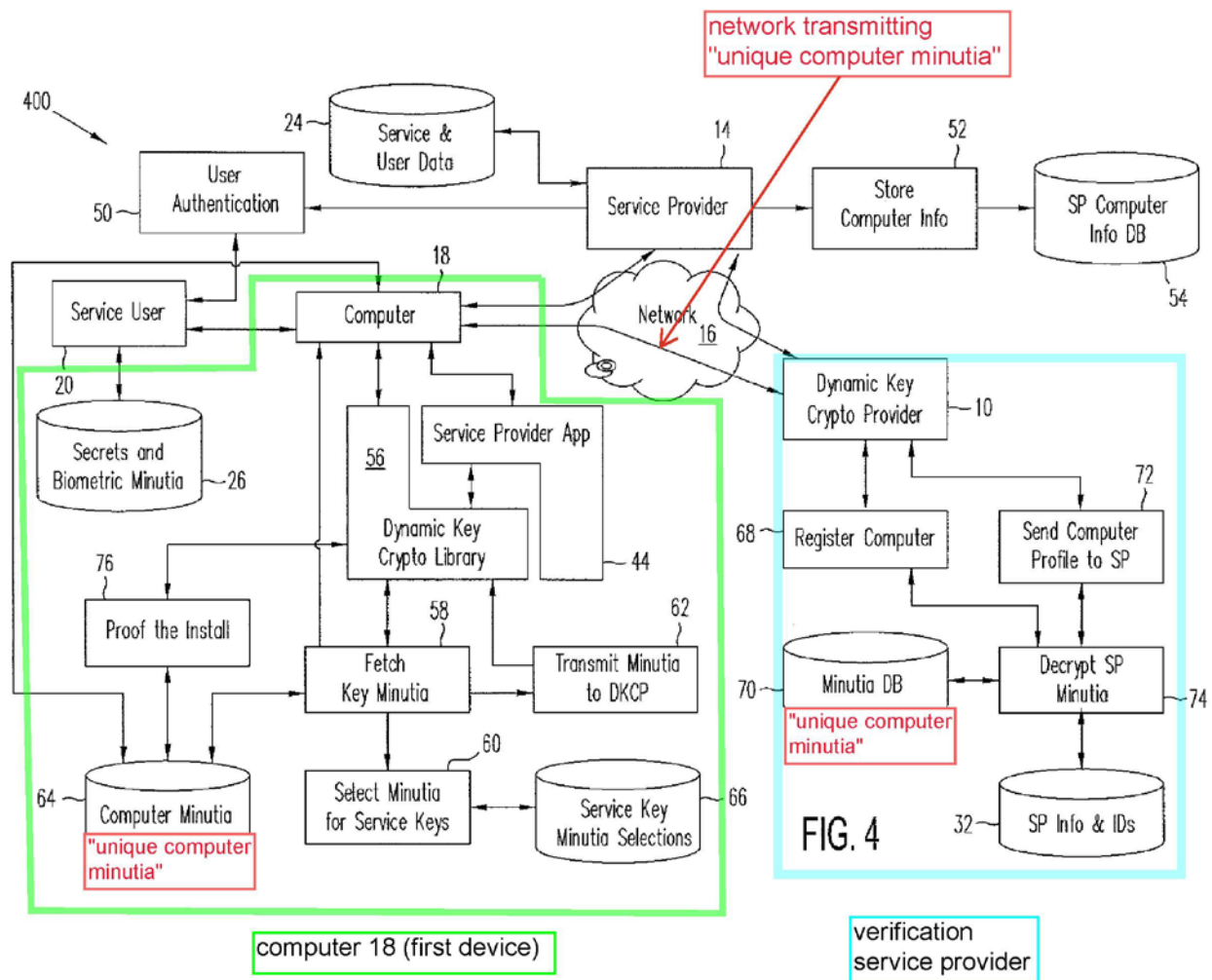
Miller describes “millions of different possible combinations of minutia DB 70 and the related practically infinite range of minutia values in the anticipated minutia DB 98” such that “each single computer 18 can be uniquely identified by matching its unique computer minutia 64...” Ex-1021, [0056]. This discloses, or renders obvious, the claimed “*device fingerprint that is generated based at least in part on a set of configuration information associated with the first device.*” Ex-1003, ¶71.

Miller “registration” describes the same process of “enrollment” using Miller’s computer minutia as is described in the (much-later) ’009 patent. For example, the ’009 patent enrolls the device with the verification service provider to store the unique device identifier:



Ex-1001, Fig. 9, 19:4-28. In the '009 patent, the device “initiates a network connection (520) deliver a unique device identifier that is then stored (522) into local storage 512 by the verification service 510. The unique identifier is also stored locally at the smartphone device.” Ex-1001, 19:19-23; Ex-1003, ¶72.

Miller’s “registration” teaches the same enrollment (at much greater detail). “FIG. 4 shows a system for registering a computer 18 with a dynamic key crypto provider 10” Ex-1021, [0085].



Ex-1021, Fig. 4. As with (the later) '009 patent, Miller's system stores the unique device identifier(s) on the device (e.g., "Computer Minutia 64" database) and on the DKCP ("minutia DB 70"). Ex-1003, ¶73.

In Miller, the computer (*first device*) includes the "dynamic key crypto library 56 [that] can sample a wide range of computer minutia 64 ... including minutiae from the computer 18 (hardware, firmware, and software)...." Ex-1021, [0089]. Miller "uses some or all of the computer minutia 64 to create encryption and identifier keys that can be used by the dynamic key crypto library 56 and other parts

of the systems.” Ex-1021, [0090]. Then, “[s]ome of the computer minutia 64 ... are sent to the dynamic key crypto provider 10 via the transmit minutia to dynamic key crypto provider (DKCP) 62 process.” Ex-1021, [0091]. This transmitted information is “unique computer minutia 64 ... that corresponds to that distinct computer 18 ... and each uniquely identified computer....” Ex-1021, [0050]; Ex-1003, ¶74.

The computer minutia are stored in “Minutia DB 70” for later use during the verification process (*store, at the verification service provider, the device fingerprint associated with the first device*):

By performing a transmit minutia to DKCP 62 process, various values of computer minutia 64 ...may be sent along with their minutia descriptor to the dynamic key crypto provider 10 which may perform a register computer 68 process. The register computer 68 process may record the computer minutia 64 and secrets and biometric minutia 26 into a minutia DB 70 along with a reference to the service provider 14 account identifier for the service user 20. The minutia DB 70 can store the type (or category) of minutia, its value and the service identifier for later processing.

Ex-1021, [0092]; [0055-0058] (describing subsequent usage); [0037] (“Collecting and registering the minutia values with the dynamic key crypto system.”). Ex-1003, ¶75.

In some embodiments, Miller may use a “hash” and/or an encrypted version of combinations of the minutia. For example, Miller describes a capability to pre-process various combinations of computer minutia that can be used for verification. Ex-1021, [0038-0039], [0051], [0065-0066], [0094], [0132-0133], [0142-0143]. This pre-processing or “hashed” versions of the minutia can be more easily and safely transmitted between the computer 18 and the DKCP. Ex-1021, [0066]; Ex-1003, ¶76.

Similarly, Miller includes an embodiment in which a cryptographic function can be applied to the sets of computer minutia used for identification / verification (at both the device and DKCP). Ex-1021, [0063-0065]. Miller references such encrypted versions as a “key” or “identifier key” which also corresponds to the *device fingerprint*. Ex-1021, [0063-0070], [0090]. Ex-1003, ¶77.

Regardless of whether it is used (or stored) in the unhashed or hashed form or whether the cryptographic function is applied, these aggregations of computer minutia are a unique device / computer identifier generated based in part on a set of configuration information associated with computer 18 (*device fingerprint that is generated based at least in part on a set of configuration information associated with the first device*). Ex-1021, Abstract (“uniquely identifying the user's electronic device using a very wide range of hardware, firmware, and software minutiae...”); [0029] (“Since the computer itself is uniquely identified, it represents a safer method

of identifying customers...”), [0050] (“each uniquely identified computer”), [0055-0056]. Furthermore, as detailed in element 1.v (and incorporated herein), the hashed (and cryptographic) versions of the device information correspond to disclosures in the ‘009 patent. Ex-1003, ¶78.

Thus, Miller’s registration process enrolls devices using the same process and same *configuration information associated with a device* as described in the ‘009 patent as a “*device fingerprint*.” The Challenged Claims issued based on this *device fingerprint* identifier (Section V.B, *supra*). Thus, Miller discloses this element and the specific element alleged to be novel during prosecution -- in far greater detail than the ‘009 patent discloses. Ex-1003, ¶79.

- v. obtain, at the verification service provider,
information transmitted by a second device
associated with a communications connection;

This element switches to the usage of the “device fingerprint” that was enrolled for the “first device” in the elements above. This element specifies that the information used for verification (in element 1.vi below) must be “transmitted by a second device.” As detailed below, Miller teaches this element when computer 18 sends a “response” containing “computer minutia” to the DKCP “indirectly via the service provider 18.” Ex-1021, [0065]; Ex-1003, ¶80.

Miller's DKCP obtains "information" to verify a first device (computer 18) communicating with Miller's service provider ("*the second device associated with a communications connection*") that provides services to computer 18 via a network. Ex-1021, [0048-0049], [0026] (Miller "enables secured actions for users of electronic computers and, more particularly, provides authentication between a client electronic computer and a service provider"). Miller's DKCP obtains the claimed "information" in the following steps. Ex-1003, ¶81.

In step 1, to verify a communication from the first device (computer 18), Miller's DKCP (verification service provider) sends a "challenge" communication to computer 18. Ex-1021, [0060-0062], [0050], [0013-0016]; Ex-1003, ¶82.

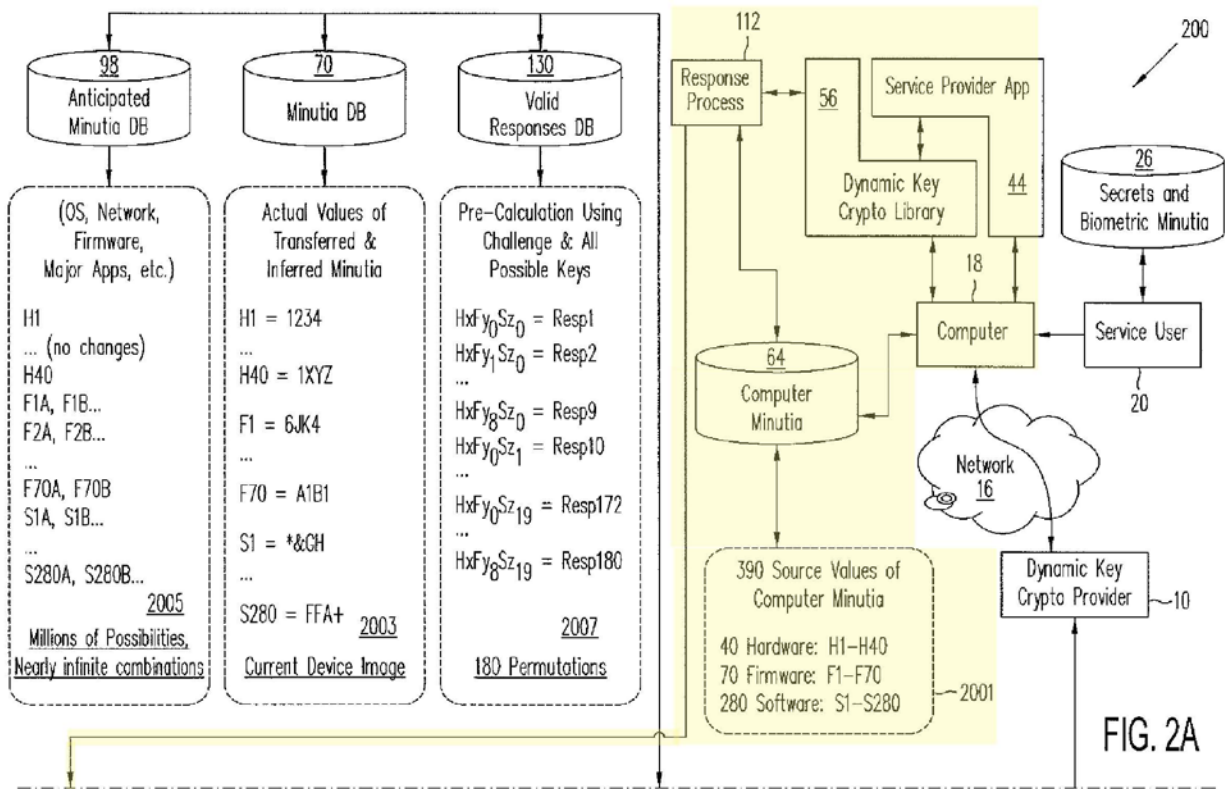
In step 2, computer 18 sends a "challenge response" contained "computer minutia" (*information*) back to the DKCP (verification service provider) indirectly through Miller's service provider ("*obtain, at the verification service provider, information ...*"). Ex-1021, Abstract, [0065], [0013-0016], [0039], [0080] ("responding to dynamic key crypto provider 10 challenges to establish a computer's unique identity..."), [0091]. As detailed in elements 1.iii, 1.iv, and 1.vi, the "information" transmitted between Miller's computer 18 and DKCP may in some embodiments be in "hashed" (pre-processed) form and/or have a cryptography function applied to it, however even in that form, it is still the information that comprises a device fingerprint as enrolled and used. Ex-1021, [0038-0039], [0051],

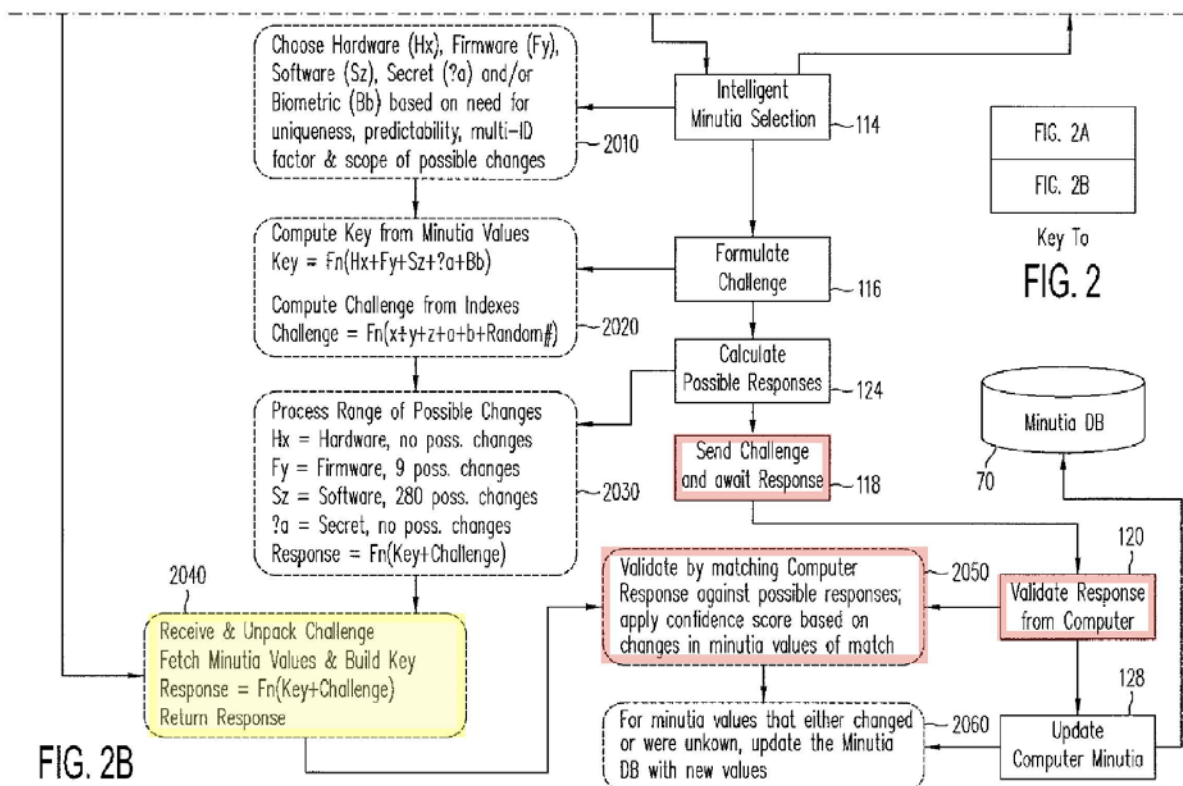
[0065-0066], [0090], [0094], [0132-0133], [0142-0143]. For example, the “hashed” version corresponds to the ‘009 disclosure in multiple manners. First, the “hashed” version is a “combination” of different minutia. Ex-1021, [0064] (noting that hashed version reflects different “permutations” of various computer minutia). This matches the ‘009 disclosure of the “device ‘fingerprint’ created from a combination of device settings, installed applications, system or application software versions, or contact list stored on the phone.” Ex-1001, 9:31-34. Just like the ‘009 disclosure, the “hashed” version is “created from a combination...” of computer minutia. Furthermore, the ‘009 patent discloses an embodiment in which device information maybe in a form similar to Miller’s cryptographic function:

For example, the response to the verification service provider can include information about the phone call being made, such as the start time of the call, device information, or a secret value or unique identifier that is known only by the device and the verification service provider. As another example, the information includes computed values that are computed, for example, using keys or codes that are known only to the device and verification provider.

Ex-1001, 15:61-16:2. The “computed values ... using keys or codes...” corresponds directly to Miller’s disclosure of the same cryptographic function being applied to the device information being exchanged between computer 18 and the DKCP. Ex-1003, ¶83.

Figures 2A/2B below show Miller's challenge / response sequence in which the computer 18 provides the "response" that includes the "computer minutia" (in various forms) used by the DKCP for verification.





Ex-1021, Figs. 2A-2B. The “computer 18” components and algorithm are highlighted in yellow. The “response process 112” uses information from the “computer minutia 64” database to formulate and “return response” as highlighted in box 2040. Ex-1021, [0064-0065]. The DKCP uses that “response” to validate the computer as highlighted by boxes 118, 120, 2050. Ex-1021, [0065-0070]; Ex-1003, ¶84.

Miller’s DKCP obtains the challenge response either directly from computer 18 or indirectly via the service provider:

At step 2040, the particular computer 18 being challenged may receive the challenge and unpack the challenge to determine which minutia it should collect and use the values of to form its response to the

challenge. ...The computer 18 being challenged may then communicate the response to return it directly to the dynamic key crypto provider 10 or indirectly via the service provider ...

Ex-1021, [0065]. Figure 1 shows the “direct” and “indirect” challenge response transmissions’ paths.

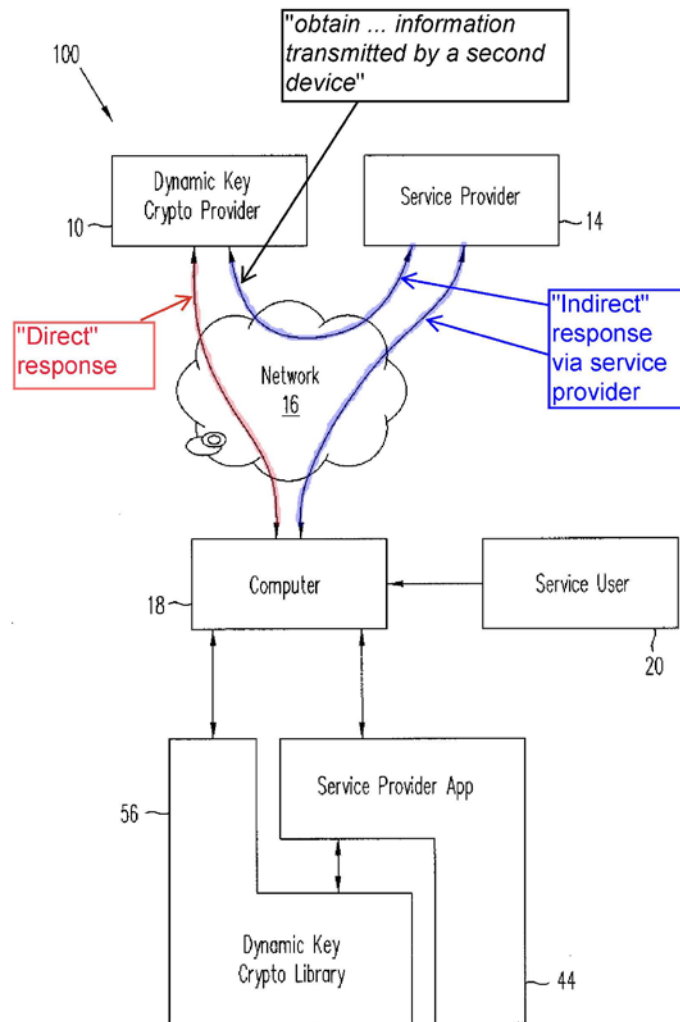


FIG. 1

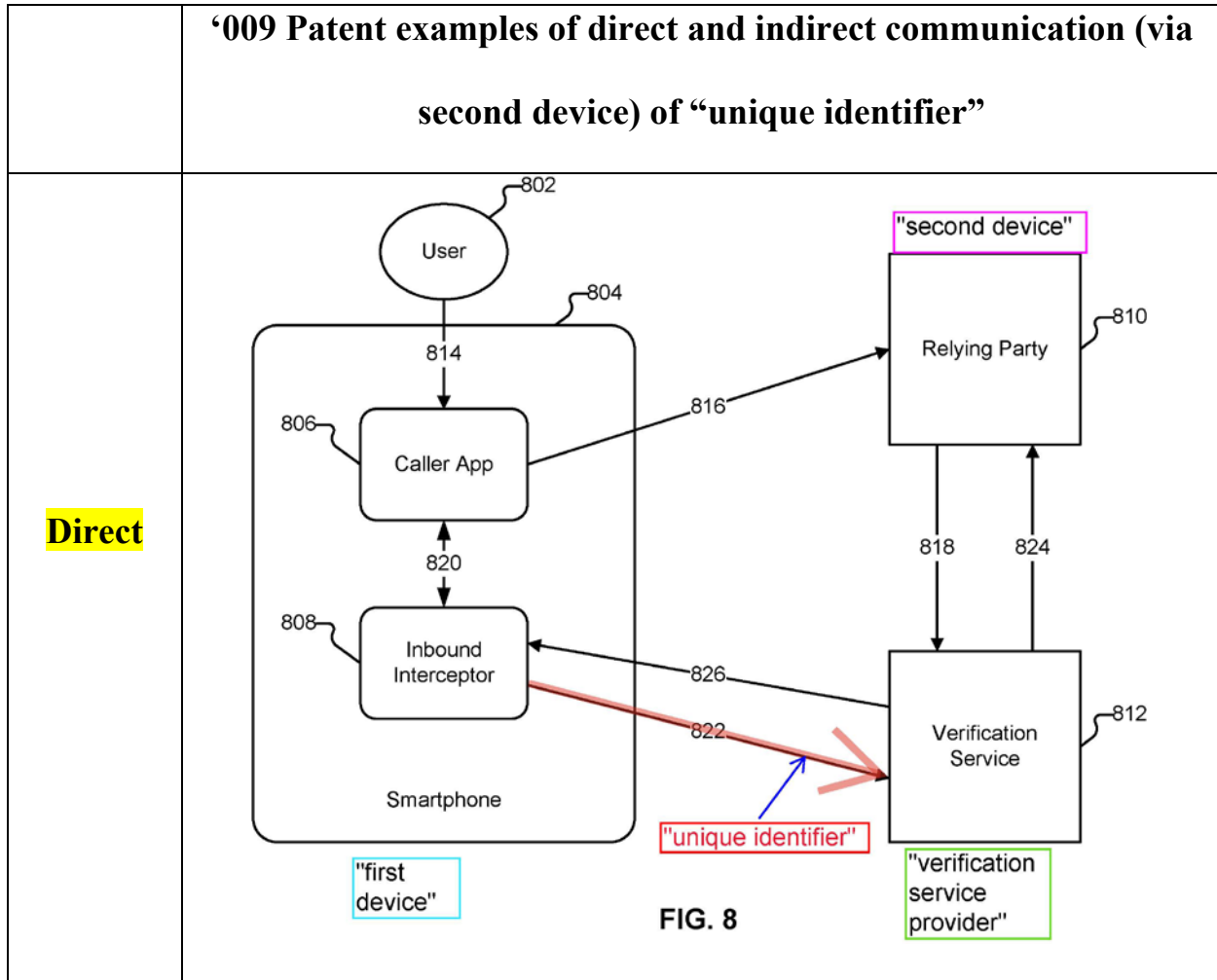
Ex-1021, Fig. 1. When the challenge response is returned “indirectly via the service provider” to the DKCP, that “response” (*information*) is being transmitted by the

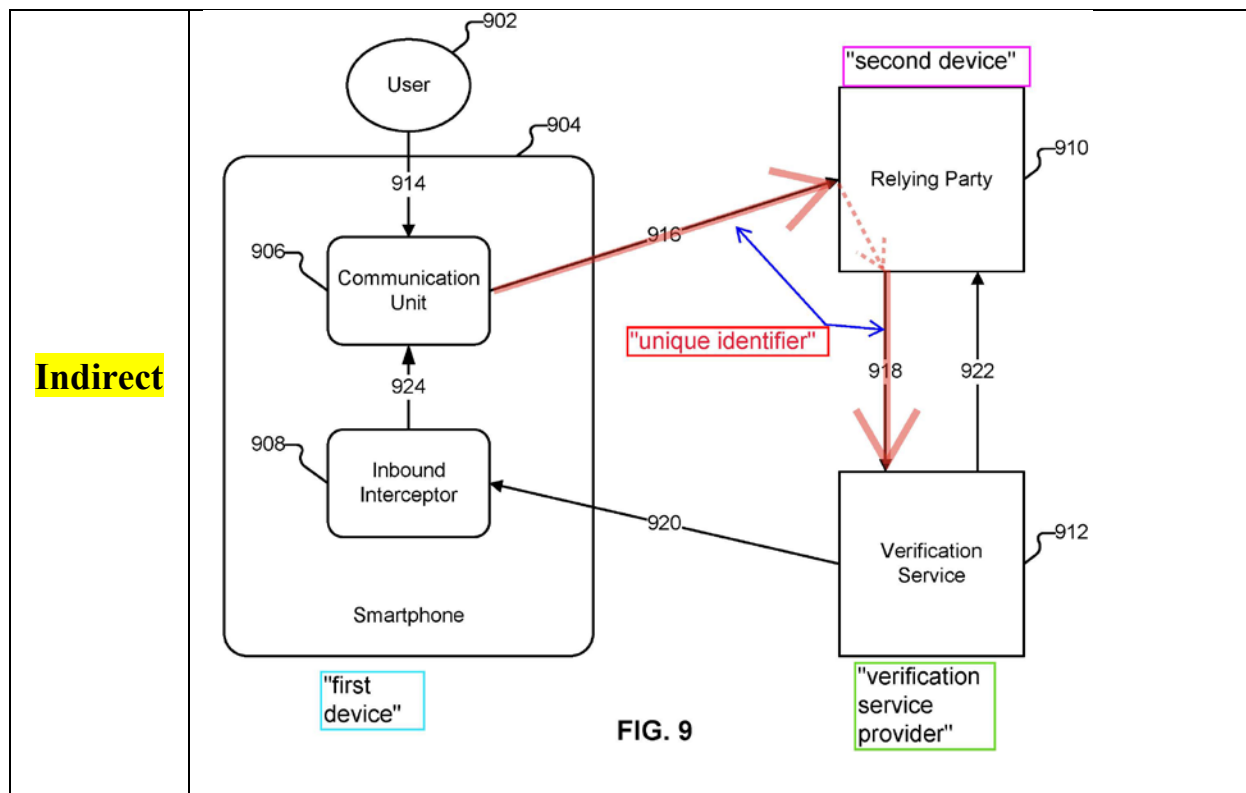
service provider (“*second device*”) – matching this claim element. *See also* Ex-1021, [0015] (“server receives an actual response to the challenge from the device”). Miller’s challenge response (*information*) can include the specific minutia, or it can include “a hash from a subset of minutia” such that “authentication can be performed as an intelligent challenge and response ... when compared to possible responses from anticipated minutiae....” Ex-1021, [0039]. *See also* Ex-1021, [0051], [0094], [0132-0133], [0142-0143]. Ex-1003, ¶85.

Moreover, even if Miller did not explicitly disclose the “indirect” transmission, it would be an obvious variation for Miller’s computer 18 to transmit information to / from the DKCP through the service provider. Such transmissions allow the computer 18 to communicate only with the service provider to simplify its communications. Moreover, the specific path of communicating the verification information to the DKCP does not impact the actual operation of verification. A POSA would recognize that any path that provides communications of the verification information can be utilized, and that the specification of such path does not provide any patentable improvement in light of known network techniques that allow for transmission of information across networks using different network nodes. Ex-1003, ¶86.

The ’009 patent subsequently used Miller’s approach of the option of direct, or indirect, communication from the “first device” to the “verification service

provider” as shown in Figure 8 (direct response) and Figure 9 (indirect response via the second device):





Ex-1001, Fig. 8 (direct), Fig. 9 (indirect). In Fig. 8, the first device directly “replies, at 822, to the verification service, with the device information.” Ex-1001, 20:27-29. In Fig. 9, the first device indirectly sends the claimed “*information*” when it “inserts the unique identifier into the already open communication channel 916 to the relying party ... [and] [t]he relying party 910 can capture the unique identifier and pass it to the verification service (912) for evaluation.” Ex-1001, 20:62-21:2; Ex-1003, ¶87.

Thus, as with the *device fingerprint* information in element 1.iii, the ‘009 patent effectively copies (and claims) Miller’s approach to *obtain, at the verification service provider, (DKCP) information* (unique identifier such as computer minutia)

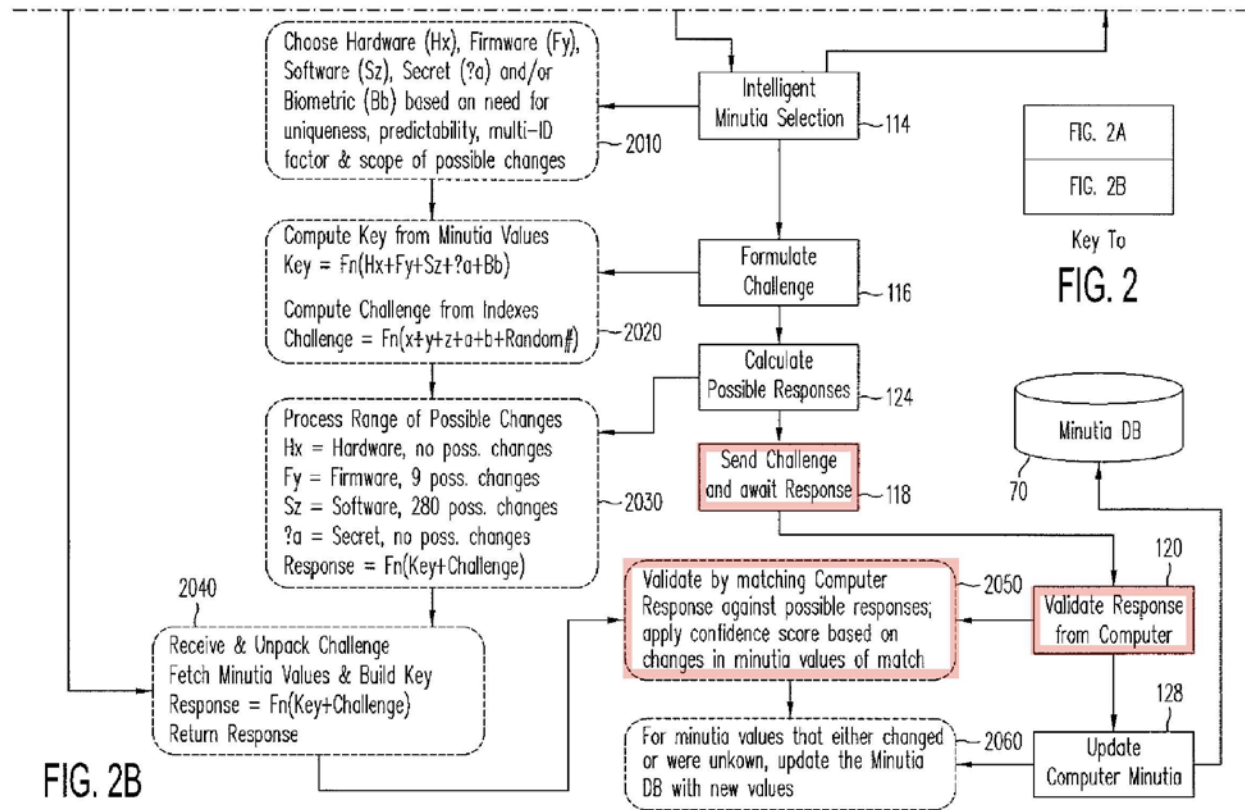
transmitted by a second device associated with a communications connection (Miller’s “service provider”). Ex-1003, ¶88.

- vi. perform, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and

The element describes the verification service provider performing a “security determination” as to whether the device that is presently communicating with the second device matches the device that was previously registered / enrolled as the “first device.” This “security determination” compares the information about the device from the registration/enrollment against the information from the first device in a communication (such as the “unique device identifier” discussed above). Based on that comparison, different actions might be selected in element 1.vii, *infra*. Ex-1003, ¶89.

Miller’s DKCP matches the minutia received in the “challenge response” from computer 18 (described in element 1.v) against the registered / enrolled minutia

stored in the DKCP database during the enrollment / registration (elements 1.iii, 1.iv). Miller's Fig. 2B shows this "matching" (element 2050) that is performed as part of the "Validate Response from Computer" (element 120):



Ex-1021, Fig. 2B.

As illustrated at step 2050, the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match.

Ex-1021, [0066]. Miller describes performing multiple different forms of matching the computer 18 response with the information stored in the DKCP minutia database.

Ex-1021, [0066-0070]. Ex-1003, ¶90.

Miller's minutia used for matching includes one or more of the "hardware minutia, Hx, one firmware minutia, Fy, and one software minutia Sz." Ex-1021, [0057]. Miller's DKCP uses combinations of "Hx-Fy-Sz" in the matching process. Ex-1021, [0066-0070]. As detailed in 1.iii, 1.iv, and 1.v, in some embodiments, Miller describes using a "hash" of the combined minutia for verification and/or applying a cryptography function. Ex-1021, [0038-0039], [0051], [0063-0070], [0094], [0132-0133], [0142-0143]. Miller's "hash" allows both the computer 18 and the DKCP to "pre-process" minutia for the response / match process and the cryptography allows for further security. Ex-1021, Abstract, [0013-0016], [0064-0066], claims 24-33. Regardless of whether the DKCP uses the hashed or unhashed minutia (or whether it is pre-processed) or whether it is subject to a cryptography function, it is still matching *information* identifying the second device against the *device fingerprint* stored by the DKCP as part of registration / enrollment. The hashing and/or cryptography provide certain additional security benefits as described in Miller, but do not change the fundamental process that the enrolled / registered device information is being compared against the information for the device presently seeking access to the service provider. Furthermore, as detailed in

element 1.v (and incorporated herein), the hashed (and cryptographic) versions of the device information correspond to disclosures in the '009 patent. Ex-1003, ¶91.

Miller's verification process matches to determine if the response from computer 18 matches the enrolled / registration information. "If a match is found, the subset of minutiae used in the challenge may be regarded as being known or authenticated." Ex-1021, [0066]. Using the hashed response from computer 18, "for example, as seen at step 2007, if the actual response matches the 172nd possible response 'Resp172' or permutation, then the actual device values must match those of Hx, the first possibility for Fy (e.g., Fy0), and the twentieth possibility for Sz (e.g., Sz19)." Ex-1021, [0066]. By attempting to match any one or more of the Hx/Fy/Sz triplet with the registered/enrolled value(s) (hashed or unhashed), Miller is *"determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device."* Ex-1003, ¶92.

In addition to the above, Miller also describes a "scoring" process used to match the minutia against the stored computer minutia information (e.g., the device fingerprint) that teaches, or renders obvious this claim element. Ex-1021, [0040], [0073], [0100], [0102-0120]; Fig. 6. Miller's DKCP includes:

Scoring the confidence of a valid response based on the minutia used Different minutia can be intelligently chosen for the challenge to achieve a response that yields a higher confidence score, increased computer uniqueness, multiple identity factors, and particular minutia isolation.

Ex-1021, [0040]. For scoring, Miller's DKCP:

receives a response validated using the subsystem 200 defined in FIG.

2. The compute score 144 process computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130, the SP info and IDs 32 data, the event log 12 and the anticipated minutia DB 98. Information in the valid responses 130 database includes both information representative of the current state of computer minutia on the computer 18...

Ex-1021, [0106], Fig. 6. Miller's DKCP uses a "vast number of minutia to be validated" including hardware, software and firmware minutia. Ex-1021, [0106-0109]. Ex-1003, ¶93.

Miller's DKCP uses hardware, software, and firmware minutia to calculate a score. After calculating a score, "the resulting score is compared against the initial threshold defined by the service provider." This process "performs a compare valid responses and threshold 152 to determine if a possible response and corresponding score are equal to or above the threshold using information from the valid responses 130 database." Ex-1021, [0113]; Ex-1003, ¶94.

Based on the comparison against various thresholds, Miller describes a process in which further information can be solicited from the computer, including information such as “biometric minutia” or other selected minutia. Ex-1021, Fig. 6B (elements 156, 158, 160, 116, 114, 170), [0111-0116]. One outcome of Miller’s scoring system is a “validation failure” resulting in service denial or re-registration.

If there is no way for a new, selected minutia challenge to achieve a score equal to or higher than the threshold requested by service provider 14, then the send validation failure to SP 162 process is performed.

When the service provider 14 receives a scoring from the Minutia validation scoring 140 from the dynamic key crypto provider 10, it first determines if a step failure 172 occurred. If this is the case, the dynamic key crypto provider 10 is unable to match the threshold desired by the service provider 14. The service provider 14 must then determine how to respond in the validation failure process 180 which, for example, can include denying the service request or conducting an out-of-band identity proofing of the service user 20 that might trigger a new computer 18 registration as shown in FIG. 4.

Ex-1021, [0117-0118]. Ex-1003, ¶95.

Miller’s “scoring” teaches, or renders obvious, the claimed “*security determination.*” First, to calculate the scores, Miller compares (matches) the computer (hardware/software/firmware) minutia received from the computer 18 against the values stored in the DKCP during registration / enrollment. Ex-1021,

[0105] (“computes a heuristic and probabilistic scoring of the minutia and minutia values used in the validated response using data from the valid responses DB 130...”). “Information in the valid responses 130 database includes [] information representative of the current state of computer minutia on the computer” as stored by the DKCP. Ex-1021, [0105]. The “[DKCP] computes all responses that are acceptable for the computer 10 to make” based upon the “minutia (*e.g.*, Hx, Fy, Sz...)” received from the device during registration and stores those valid responses in the “valid responses DB.” Ex-1021, [0064]. Thus, the process of “comput[ing]” Miller’s score teaches or renders obvious, the claimed matching because it “determin[es] whether the obtained information ... matches at least a portion of” Miller’s computer information stored in the DKCP during registration. Ex-1003, ¶96.

Furthermore, Miller’s “scoring” matches an embodiment of the (much later) ’009 patent using “scoring” for validity. Ex-1001, 10:57-60 (“As the confirmation data is received (*e.g.*, by the verification service), it is verified against the information that was previously stored for the user’s device at the verification service using, for example, the scoring described above.”), 9:34-10:20, 12:10-23. Ex-1003, ¶97.

Miller’s scoring system mirrors the ’009 scoring system in which “the device information is combined with other information” in which “the verification score is

created using a variety of approaches.” Ex-1001, 9:34-50. If the score is not high enough, then the Miller’s DKCP challenges the device to obtain more authentication minutia for scoring as detailed above. In the ‘009 patent, just as Miller did, “the relying party incorporates the score into a risk-based decision system...” Ex-1001, 9:45-47. Analogously, based on the score, the ‘009 patent “decision system then selects from a range of appropriate responses, which include at least one of blocking access, requesting additional authentication factors, permitting access, etc.” Ex-1001, 9:51-54; Ex-1003, ¶98.

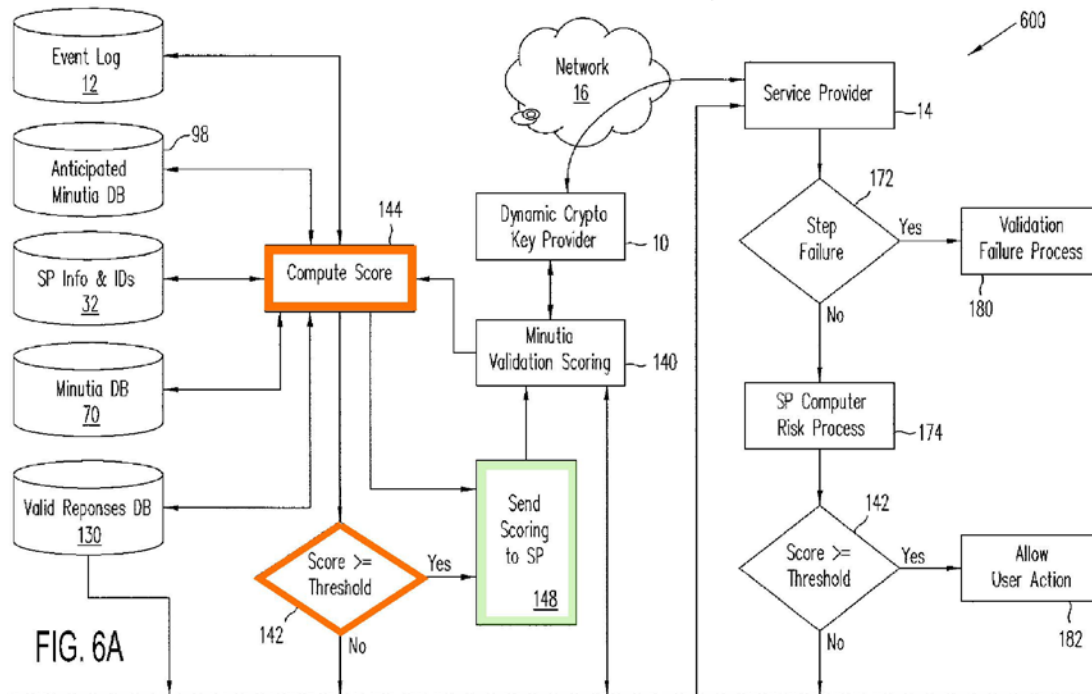
Further evidence that Miller’s “scoring” system discloses, or renders obvious, the claimed “security determination” in the ‘009 patent appears from child patents to the ‘009 patent. For example, the ‘989 child patent includes claims that recite “perform a security determination based at least in part on the score generated for the calling device.” Ex-1022, Claim 1. Claims 11 and 12 of the ‘989 patent similarly describe a “score ... generated based ... on device information” – just like Miller teaches. Ex-1003, ¶99.

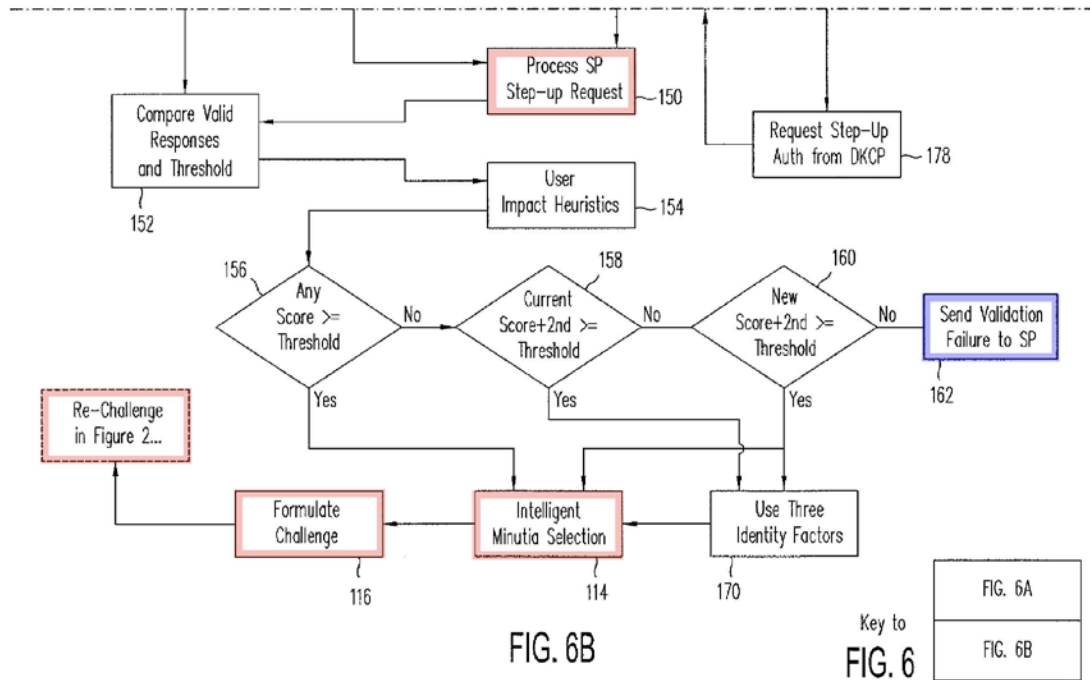
Thus, Miller teaches, or renders obvious, performing a security determination as recited in this element. Ex-1003, ¶100.

- vii. based at least in part on the security determination, select an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.

Miller's system teaches, or renders obvious, all three of the claimed actions based on the security determination described in 1.vi. Ex-1003, ¶101.

First, Miller's DKCP may “select an action comprising ... requesting additional authentication” in multiple ways. First, as detailed for 1.vi, the DKCP may compute and assess the score against a “threshold” as shown in blocks 144, 142 below. Ex-1021, [0112-0116]; Ex-1003, ¶102.





If the “score $\geq$ threshold” check in block 142 fails, the DKCP may perform a “SP step-up request 150 process” which leads to the DKCP performing a “re-challenge in Figure 2” to obtain additional information. Ex-1021, Fig. 6B; [0114]. Ex-1003, ¶103.

As shown in blocks 114 and 170 above, this “re-challenge” process may include both “intelligent minutia selection” and “three identity factor” selection. Ex-1021, [0061-0062], [0115]. The “three identity factor” minutia may “direct” the system “to collect service user 20 secrets or biometric minutia using computer 18” for additional authentication (beyond computer minutia) using a “three identity factor” authentication. Ex-1021, [0115]. A three-identity factor uses “the three factors of identity (‘have’, ‘know’, and ‘are’, e.g., respectively, the computer 18, the secrets service user 20 knows or represents or biometric minutia (from secrets and

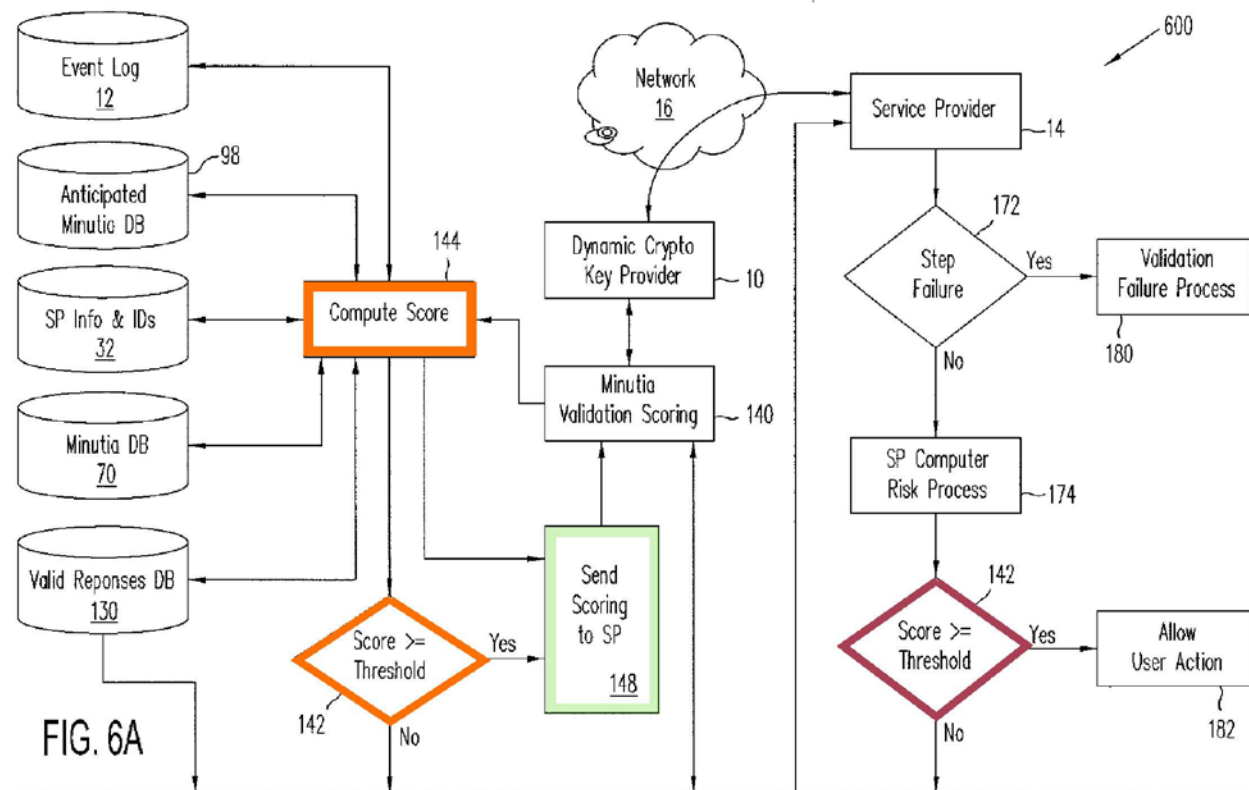
biometric minutia 26)).” Ex-1021, [0132]; *See also* Ex-1032, [0031], [0121], Fig. 7. For the additional authentication using “secrets service user 20 knows,” Miller describes “secrets a user of the computing device knows (e.g., a PIN number or password).” Ex-1021, [0031]. Ex-1003, ¶104.

Miller’s request for additional authentication information, such as user-known information, matches the (later) ‘009 patent’s disclosure. For example, the ‘009 patent describes “additional authentication tools including PIN verification, password verification” – exactly matching Miller’s user secrets used in the re-challenge for additional authentication discussed above. Ex-1001, 13:11-12; Ex-1003, ¶105.

Miller also teaches or renders obvious to “*select an action comprising ... blocking the communication.*” Miller’s DKCP evaluates the computer’s “challenge response” as detailed above. “If the response is not an expected response, then a validation failure process as described in FIG. 6B can alert the service provider 14 that the validation has failed.” Ex-1021, [0069]. Similarly, based on the scoring not meeting a threshold, Miller’s DKCP may select the action of “send[ing] validation failure to SP 162 process.” Ex-1021, [0117]. Both types of “validation failure” can result in “denying the service request” which teaches “*select[ing] an action comprising at least one of blocking the communication.*” Ex-1021, [0118]. At a minimum, given that Miller expressly teaches a logic path in which the result is

“denying the service request,” it would be obvious that such denial would be effectuated by selecting an action blocking the communication because such blocking is one known way of such denial. Ex-1003, ¶106.

Miller discloses “*permitting the communication*” in multiple passages. For example, based on the security determination in 1.vi, “[i]f the computed score $\geq$ threshold 142 then the send score to SP 148 process is used to return the score to the service provider 14 for further consideration.” Ex-1021, [0111]. This is shown below in which the DKCP is computer and evaluating the score (orange) and then, if “score $\geq$ threshold” then sending the score to the service provider (green box 148).



Ex-1021, Fig. 6A.³ Miller’s DKCP characterizes this threshold as the DKCP “minimum scores to allow connection” – further bolstering that this evaluation is the claim security determination. Ex-1021, [0073]. Ex-1003, ¶107.

For the “blocking” and “permitting” selected actions above, Miller’s teaching is primarily that the “service provider” (and not the DKCP) performs the actual denial (block) or allow (permit). However, Miller still discloses or renders obvious this claim. First, the claim recites “select an action...” but the claim does not recite that the verification service provider must perform the selected action. Miller’s DKCP teaches, or renders obvious, this element when the DKCP selects the action, and informs Miller’s “service provider” of the selected action. Second, Miller operates exactly how the ‘009 patent operates. In the ‘009 patent, “the verification service creates a verification score.” Ex-1001, 9:38. Then, “the relying party incorporates the score into a risk-based decision system” – which matches Miller’s teaching that the “relying party” (e.g., the claimed second device / Miller’s “service provider”) uses the calculated score. Ultimately, “[t] decision system then selects from a range of appropriate responses, which include at least one of blocking access, requesting additional authentication factors, permitting access, etc.” Ex-1001, 9:46-

³ The service provider then separately evaluates the score (in purple). “If the score>=threshold 142 then the allow user action 182 may be performed.” Ex-1021, [0119], Fig. 6A.

54. The “relying party” in the ‘009 patent corresponds to Miller’s “service provider.” Ex-1003, ¶108.

Thus, Miller’s service provider using the DKCP score to perform the block/allow action matches the ‘009 patent disclosure in which the “decision system” in the second device (relying party) uses the score for the actions. Ex-1003, ¶109.

Third, in the ‘009 embodiments correspond to the claim (*e.g.*, Figs. 8 and 9 and their disclosure), the “verification service” does not sit in the communication path between the first and second devices. The verification service does not have any practical operation to block / allow the call (likely the reason the claim only requires to “select” the action, not to perform it). Ex-1003, ¶110.

Thus, Miller discloses, or renders obvious, this element – particularly in light of the heavy overlap between the ’009 patent disclosure and Miller. Ex-1003, ¶111.

b. Claim 2:

The system of claim 1, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.

Miller discloses, or renders obvious, this claim in two distinct fashions. First, this claim apparently further clarifies element 1.v in that the verification service

provider will “obtain” the “information” through a particular channel. As shown in Miller’s Fig. 1, the channel / path between the “computer 18” and the “service provider” is different from the channel / path on which the DKCP obtains the information transmitted by the second device.

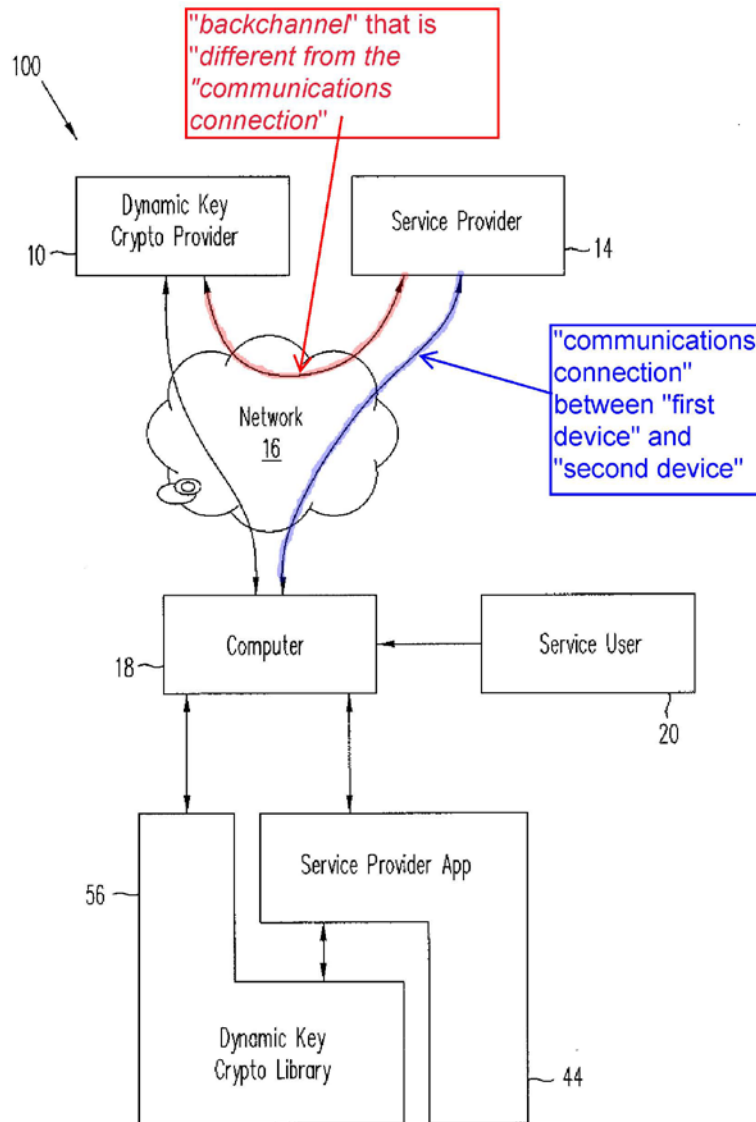


FIG. 1

Ex-1021, Fig. 1. While Miller's transmissions are shown across the same "network," Miller does not ever recite that the two separate transmissions are on the same connection. Ex-1003, ¶112.

Second, Miller's system matches the description of a "backchannel" in the '009 patent stating:

[T]he channel that is used for the verification service request to the calling device is different from the initial, primary communication channel used by the calling device to make the call (e.g., a separate, different backchannel is used to make the verification service request).

Ex-1001, 15:41-46. In Miller, the "challenge" to the computer 18 (calling device) corresponds to the '009 patent's "verification service request to the calling device." Miller's "challenge" is transmitted on the path between the DKCP and the computer 18, as detailed in 1.v. As in Miller, in the '009 patent, this "verification service request" can be sent on a separate communication channel from the verification service "to the calling device." Ex-1001, Fig. 9; Ex-1003, ¶113.

The "*information transmitted by the second device is obtained via*" this channel because this challenge causes Miller's "challenge response." As detailed in 1.v, that "challenge response" can be indirectly transmitted through the service provider in Miller, just as the "information" is received indirectly in the '009 patent through the callee device. Ex-1001, Fig. 9; Ex-1003, ¶114.

Thus, Miller describes the same “backchannel that is different from the communications connection” as is disclosed in the ’009 patent.

c. Claim 3

The system of claim 1, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.

Miller teaches, or renders obvious, such an assurance. For example, as detailed in element 1.vii, the security determination includes the score / threshold comparison. “If the computed score $\geq$ threshold 142 then the send score to SP 148 process is used to return the score to the service provider” which then may allow the user action because “the confidence in the computer 18 ...may be sufficient for the service provider 14 to allow the requested action.” Ex-1021, [0111], [0119], Fig. 6A. In contrast, if the score does not meet the threshold, then then DKCP may perform other actions, such as evaluate other minutia as detailed in element 1.vii and/or invoke the “validation failure” 180 process. Ex-1021, Figs. 2A-2B, 6A-6B. Ex-1003, ¶116.

The '009 patent description of “assurance” matches Miller’s. E.g., Ex-1001, 10:57-64 (“the verification service using ... the scoring” and “then an assurance is produced and conveyed to the callee....”). Ex-1003, ¶117.

The “allow user action” communication and the communication of the score (which only occurs if the threshold test passes) from DKCP to the service provider (“*recipient associated with the communications connection*”) is thus an “assurance.” Ex-1003, ¶118.

d. Claim 4

The system of claim 1, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.

Miller discloses, or renders obvious, this element. In Miller, as detailed in claim 5, computer 18 may be a “mobile phone” such that the “phone numbers” can be used for the identification as one of the “minutia” used for verification. Ex-1021, [0026], [0048], [0051], [0067]. The “network” used for communication includes a “mobile operator network.” Ex-1021, [0097]. At a minimum, it would be obvious that a communication from a “mobile phone” over a “mobile operator network” would be a “phone call.” The communications would be a “phone call” even if the other end of the communication was a service provider “website” because

communications from mobile phones can be considered a “data” phone call. Indeed, the ’009 patent articulates “audio” calls when it so requires such a call. Ex-1001, 15:46-48. Ex-1003, ¶119.

Miller also teaches that the network used for communication is the “PTSN” (an apparent misspelling of “PSTN”). Ex-1021, [0182]. The “PSTN” is the “public switched telephone network.” Communications across the PSTN would be “phone calls.” An example in Miller of such a communication would be a “personal computer” using a “modem” to communication across a PSTN to a service provider. Ex-1021, [0177-0178]. Ex-1003, ¶120.

Moreover, computer 18 includes “email” capabilities. Ex-1021, [0056]. A POSA would understand such capabilities render obvious that the communication is an email. Ex-1003, ¶121.

e. Claim 5

The system of claim 1, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.

Miller’s “computer 18” includes “a mobile phone, computer system, smart phones, laptops, tablets....” Ex-1021, [0048]; Ex-1003, ¶122.

f. Claim 6

The system of claim 1, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.

Miller discloses, or renders obvious, this element. Element 1.iii details Miller's DKCP registering computer 18 to store minutia used for later verification of computer 18 ("enrolling the first device"). *See* 1.iii (citing, e.g., Ex-1021, [0085-0094], Fig. 4). Included in the registered minutia used for verification, Miller describes a wide variety of "secrets a user of the computing device knows (e.g., a PIN number or password)..." Ex-1021, [0031], [0054], [0094]. Miller's "FIG. 7 shows a system ... using minutiae from the three identity factors (have, know and are) found on computer 18 or collected from a service user 20" such as "[w]hen a PIN or password entry is required..." Ex-1021, [0121-0122]. Miller details procedures for entering and using a PIN / password. Ex-1021, [0121-0133]. Ex-1003, ¶123.

Miller teaches that the registration "*is based at least in part on at least one of PIN verification [and] password verification.*" For example, Miller's registration

process includes a “user authentication 50 process” in which “the service user 20 might answer previously defined questions... or other identity proofing methods.” Ex-1021, [0086]. Given that Miller notes “[t]he standard method for identifying a user to an online service is by entering a username and password,” (Ex-1021, [0010]) it would be at least obvious that the “user authentication 50 process” would include the “standard method” which involves PIN/password verification. Ex-1003, ¶124.

Moreover, it would also be obvious that the “identity proofing methods” would include the PIN and password verification that Miller identifies as “identity factors.” Ex-1021, [0031] (“secrets a user of the computing device knows (e.g., a PIN number or password)”), [0128] (“When a PIN or password entry is required, for example, as a second identity factor ...”), [0028]. Moreover, given that Miller teaches after “user authentication,” the registration continues. Ex-1021, [0088]. Thus, Miller teaches, or renders obvious, the use of PIN or password verification. Ex-1003, ¶125.

Miller also describes an iterative process in which a “relatively small amount of computer minutia 64 and secrets and biometric minutia 26 can be sent to the dynamic key crypto provider 10 so the dynamic key crypto provider 10 can look for existing matches to the computer minutia 64 in its minutia DB 70 database. If the dynamic key crypto provider 10 finds matching minutia 64, then the dynamic key crypto provider 10 can send challenge, response, and validation exchanges described

in FIG. 2 to verify a wider set of computer minutia.” Ex-1021, [0091]. Ex-1003, ¶126.

Miller teaches, or renders obvious, “*a check of at least one of a name, an address, and a phone number*” as part of the registration process. For example, Miller’s DKCP checks the “account identifier” during registration:

When a new computer 220 performs the registration system 400 shown in FIG. 4, if the dynamic key crypto provider 10 discovers that the account identifier supplied by the service provider 14 is already in use by a similar computer 18 (for example, a second smart phone) then a transfer service 238 message can be added as part of the registration process.

Ex-1021, [0156]. In Miller, it is the “account identifier that the service provider 14 uses to identify the service user 20.” Ex-1021, [0088]; see also Ex-1021, [0092] (“account identifier for the service user”). Because the “account identifier” identifies a user (a person), it would be an obvious that such account identifier includes a name (including a “username”). For example, Miller teaches “[t]he standard method for identifying a user to an online service is by entering a username and password.” Ex-1021, [0010]. Thus, it would be at least obvious that an “account identifier” that “identifies the service user” teaches using a “username” which is the “standard method for identifying a user.” *Id.*; Ex-1003, ¶127.

Therefore, Miller's *enrolling* (registering) *the first device is based at least in part on ... a check of at least a name* (username)." Ex-1003, ¶128.

g. Claim 7

The system of claim 1, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.

As detailed above, Miller teaches an additional authentication that includes PIN and/or password verification in checking the "minutia" for verification. See elements 1.vi, 1.vii; claim 6. For example,

Nearly any data can be introduced into the system 200 by the definition and addition of minutia classes. For example, PIN, password, service history and other service user 20 secrets can be entered and processed as if they were a class of minutia... a PIN screen can be displayed on the computer 18, the service user 20 can enter their PIN (or other secret value) and the information entered can be processed as the minutia value in the method here described by system 200.

Ex-1021, [0054]. As detailed above, any form of minutia can be used in Miller's "challenge" to the computer 18 and returned in the "response" that is verified / matched against the DKCP's minutia databases. Miller teaches "forcing a user to enter a ... computer PIN ... on a registered computer to include user minutia... to ensure a value user is controlling [the] computer." Ex-1021, [0044]. See elements 1.vi, 1.vii, claim 6 (detailed various minutia and the processing thereof). Ex-1003, ¶129.

Furthermore, Miller teaches that, in addition to the normal authentication (using, for example, "computer minutia" as described in element 1.vi), certain communications from the user to the service provider can require a PIN verification:

Should a user's online activities require an even higher level of trust, the platform (e.g., dynamic key crypto service and related client software) can force the user to enter the user's standard PIN into the computer to ensure a valid user is the person using the computer.

Ex-1021, [0029]. *See also* Ex-1021, [0028] ("the user can be asked to enter a second identity factor such as a secret PIN ... into the computer only if required by the service"), [0073] (registration preference to "use a service PIN."); [0044] ("forcing a user to enter a service PIN, computer PIN ... to ... ensure a valid user is controlling an identified computer"); [0122-0129] (describing the forcing of a "PIN" to further authenticate the user as shown in Fig. 7); Fig. 7; [0060] ("user secrets" which includes PIN and password). Ex-1003, ¶130.

Miller also teaches that the additional authentication can include the “minutia” of “geo-location.” Ex-1021, [0031] (“Other minutia may include such information as geo-location from GPS (global positioning system) capability of the computing device”), [0040], [0051], [0060] (“Minutia sets can be selected to address specific purposes such as geo-location or user secrets”), [0133], claims 7, 14. Ex-1003, ¶131.

Miller’s DKCP can use “*phone numbers*” as part of the authentication process (and thus part of the “additional authentication” beyond the use of the “device fingerprint” as described in elements 1.vi, 1.vii). For example, during “collection of minutia” (used by the DKCP), “phone numbers can be hashed.” Ex-1021, [0051]; see also Ex-1021, [0067] (a “validate response ... can employ multiple methods of collecting ... a smartphones phone number” or a “phone number” in the “returned minutia.”). This teaches that “phone numbers” are part of the minutia that is collected and used for authentication, including the “additional authentication” in the process in Fig. 2 described in elements 1.vi, 1.vii. Ex-1003, ¶132.

Furthermore, the minutia used for additional authentication can “*comprise ... a check of ... a phone number* in another fashion by using “contact phone numbers” as minutia in the authentication process described in elements 1.vi, 1.vii. Ex-1021, [0052], [0056] (“the minutiae that can be collected from the computer 18 (e.g., frequently called phone numbers)”), [0056] (added “contacts... [are] customizations ... (i.e. minutia) [that] can immediately differentiate two examples of compute”). A

POSA would understand “contacts” to include “contact phone numbers” in light of Miller’s disclosures. Ex-1003, ¶133.

Relatedly, Miller’s authentication (including additional authentication) can “*comprise ... a check of ... an address.*” For example, Miller’s DKCP may include “values in the minutia DB” that are checked to see if addresses in “an address book” change over time for validation. Ex-1021, [0099]. Ex-1003, ¶134.

Thus, given that Miller specifically teaches the claimed data (such as PIN, password, address, phone number...) as identified above can be “minutia” used for authentication, and Miller teaches that the challenge process can ask for any type of additional minutia to be provided by the computer 18 and checked by the DKCP, Miller teaches, or renders obvious this claim. Ex-1003, ¶135.

h. Claim 8

The system of claim 1, wherein the set of configuration information comprises at least one of a set of device settings, a set of installed applications, system version information, application software version information, and a contact list associated with the first device.

As detailed in element 1.iii, Miller’s sets of computer minutia (*configuration information*) comprises at least one of a set of “which firmware and software codes

are installed on the computing device and characteristics such as what particular version or release date of firmware or software are installed on the computing device” as well as firmware/software “version number, revision number” and the “contacts” and ‘contact phone numbers. *See* 1.iii (citing Ex-1021, [0031]. [0052], [0055-0056]). Miller’s computer minutia includes device settings. Ex-1021, [0031] (“make and model of the computing device or a circuit manufacturer's ID number”); [0052] (“device manufacturer, model number, serial number...”). Ex-1003, ¶136.

i. Claim 9

The system of claim 1, wherein the verification service provider is further configured to re-enroll the first device in response to a determination of a change in the device fingerprint.

Miller’s DKCP performs an update to re-register computer 18 in response to a determination that the computer minutia from computer 18 have changed – which corresponds to this claim. Indeed, as an initial matter, Miller acknowledges that such re-enrollment was already known in the art even before Miller. Ex-1021, [0011]. In explaining the how “computer fingerprints” are based upon configuration information on the computer device, Miller notes that was already known that “changes to the minutia on a unique computer occur naturally during normal use and can invalidate the computer fingerprint process or inconvenience the user or service

by forcing a re-initialization of the computer fingerprint.” Ex-1021, [0011]. Thus, Miller discloses, or renders obvious, this element in its background discussion of known art. Miller further discloses this claimed re-enrollment in multiple fashions. Ex-1003, ¶137.

First, when evaluating the device fingerprint returned in the response from the computer 18, “if an exact match is not found ... changes in the computer minutia 64 of a computer 18 can be sent from the computer 18 to the dynamic key crypto provider 10 using the registration subsystem 400 described in FIG. 4.” Sending the “changes in the computer minutia” to the DKCP “using the registration system” teaches, or renders obvious, the claimed re-enrollment. The purpose of sending such changes via the registration system is to ensure that the DKCP has the correct, current version of the computer minutia (device fingerprint) to allow for verification of the computer 18. The DKCP’s detection that the DKCP version of the computer minutia (which was previously registered by computer 18) does not now match the computer minutia received from computer 18 is a “*determination of change in the device fingerprint.*” As detailed above, updating the computer minutia (using the registration process) reflects that the DKCP *re-enrolls the first device* (computer 18) *in response to the determination* (mismatch). Ex-1003, ¶138.

Second, in Miller’s DKCP, “[i]f the response [from computer 18] is not an expected response [according to the DKCP’s databases established during

registration], then a validation failure process as described in FIG. 6B” is invoked. Ex-1021, [0069]. The “validation failure” may cause “conducting an out-of-band identity proofing of the service user 20 that might trigger a new computer 18 registration as shown in FIG. 4.” Ex-1021, [0118]. Thus, in this example, the DKCP determines that the device fingerprint has changed because the received computer minutia response no longer matches the computer minutia received during registration with the DKCP. “In response to” this determination, the DKCP identifies a “validation failure” resulting in a re-registration – thus meeting this claim. Ex-1003, ¶139.

Third, the “validation failure” can also be caused by low “scores” calculated based upon the match (or mismatch) of computer minutia in the response against that minutia stored in the DKCP database during registration. Ex-1021, [0117-0118]. This form of “validation failure” also can cause the same re-registration discussed above. Ex-1003, ¶140.

Thus, Miller teaches, or renders obvious, this element. Ex-1003, ¶141.

j. Claim 10

Claim 10 is merely the method claim corresponding to the system in claim 1 and is invalid based upon the same reasoning above. Claims 11-16 also correspond to dependent claims from system claim 1 and are invalid for the same reasons as for the correspond system dependent claims. Ex-1003, ¶142.

- i. A method, comprising:

If the preamble is limiting, Miller discloses “a method” in using the system described in claim 1. Ex-1003, ¶143.

- ii. enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;

Miller discloses this limitation for the same reasons as Claim 1(ii)-1(iii). Ex-1003, ¶144.

- iii. storing, at the verification service provider, the device fingerprint associated with the first device;

Miller discloses this limitation for the same reasons as Claim 1(iv). Ex-1003, ¶145.

- iv. obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;

Miller discloses this limitation for the same reasons as Claim 1(v). Ex-1003, ¶146.

- v. performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and;

Miller discloses this limitation for the same reasons as Claim 1(vi). Ex-1003, ¶147.

- vi. based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the

communication, requesting additional authentication, and permitting the communication.

Miller discloses this limitation for the same reasons as Claim 1(vii). Ex-1003, ¶148.

k. Claim 11

The method of claim 10, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.

Miller discloses this limitation for the same reasons as Claim 2. Ex-1003, ¶149.

l. Claim 12

The method of claim 10, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a recipient associated with the communications connection.

Miller discloses this limitation for the same reasons as Claim 3. Ex-1003, ¶150.

m. Claim 13

The method of claim 10, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.

Miller discloses this limitation for the same reasons as Claim 4. Ex-1003, ¶151.

n. Claim 14

The method of claim 10, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.

Miller discloses this limitation for the same reasons as Claim 5. Ex-1003, ¶152.

o. Claim 15

The method of claim 10, wherein enrolling the first device is based at least in part on at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation,

and a check of at least one of a name, an address,
and a phone number.

Miller discloses this limitation for the same reasons as Claim 6. Ex-1003,
¶153.

p. Claim 16

The method of claim 10, wherein the additional authentication comprises at least one of PIN verification, password verification, knowledge-based authentication, geolocation information, credit card information validation, and a check of at least one of a name, an address, and a phone number.

Miller discloses this limitation for the same reasons as Claim 7. Ex-1003,
¶154.

q. Claim 17

Claim 17 is merely the computer program product claim corresponding to the system in claim 1 and is invalid for the same reasons. Claims 18-23 correspond to dependent claims from system claim 1 and are invalid for the same reasons as for the corresponding system dependent claims. Ex-1003, ¶155.

- i. A computer program product embodied in a tangible and non-transitory computer readable storage medium and comprising computer instructions for:

If the preamble is limiting, Miller's DKCP operates using "[l]ogic ... encoded in a computer readable and executable medium ... providing instructions to the processor for execution." Ex-1021, [0180]. See also Ex-1021, [0177-0185], claims 30-34; Ex-1003, ¶156.

- ii. enrolling a first device with a verification service provider, wherein enrolling the first device includes associating, by the verification service provider, the first device with a device fingerprint that is generated based at least in part on a set of configuration information associated with the first device;

Miller discloses this limitation for the same reasons as Claim 1(ii)-1(iii). Ex-1003, ¶157.

- iii. storing, at the verification service provider, the device fingerprint associated with the first device;

Miller discloses this limitation for the same reasons as Claim 1(iv). Ex-1003, ¶158.

- iv. obtaining, at the verification service provider, information transmitted by a second device associated with a communications connection;

Miller discloses this limitation for the same reasons as Claim 1(v). Ex-1003, ¶159.

- v. performing, at the verification service provider, a security determination at least in part by determining whether the obtained information transmitted by the second device matches at least a portion of the stored device fingerprint that was generated based at least in part on the set of configuration information associated with the enrolled first device; and;

Miller discloses this limitation for the same reasons as Claim 1(vi). Ex-1003, ¶160.

- vi. based at least in part on the security determination, selecting, at the verification service provider, an action comprising at least one of blocking the communication, requesting additional authentication, and permitting the communication.

Miller discloses this limitation for the same reasons as Claim 1(vii). Ex-1003, ¶161.

r. Claim 18

The computer program product of claim 17, wherein the information transmitted by the second device is obtained via a backchannel that is different from the communications connection.

Miller discloses this limitation for the same reasons as Claim 2. Ex-1003, ¶162.

s. Claim 19

The computer program product of claim 17, wherein based at least in part on the security determination, the verification service provider is further configured to convey an assurance to a

recipient associated with the communications connection.

Miller discloses this limitation for the same reasons as Claim 3. Ex-1003,

¶163

t. Claim 20

The computer program product of claim 17, wherein the communications connection is associated with at least one of email, SMS, instant message, and a phone call.

Miller discloses this limitation for the same reasons as Claim 4. Ex-1003,

¶164.

u. Claim 21

The computer program product of claim 17, wherein the first device comprises at least one of a smartphone, a tablet, a PC, a phablet, and a wearable device.

Miller discloses this limitation for the same reasons as Claim 5. Ex-1003,

¶165.

v. Claim 22

The computer program product of claim 17,
wherein enrolling the first device is based at least
in part on at least one of PIN verification,
password verification, knowledge-based
authentication, geolocation information, credit card
information validation, and a check of at least one
of a name, an address, and a phone number.

Miller discloses this limitation for the same reasons as Claim 7. Ex-1003,
¶166.

w. Claim 23

The computer program product of claim 17,
wherein the additional authentication comprises at
least one of PIN verification, password
verification, knowledge-based authentication,
geolocation information, credit card information
validation, and a check of at least one of a name,
an address, and a phone number.

Miller discloses this limitation for the same reasons as Claim 7. Ex-1003, ¶167.

VIII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER *FINTIV*

In *Apple Inc. v. Fintiv, Inc.*, the Board set forth six non-dispositive factors to guide whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued interim procedure regarding application of the *Fintiv* factors (Interim Guidance) stating that “the PTAB will not deny institution of an IPR or PGR under *Fintiv* [] when a petition presents compelling evidence of unpatentability.” USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA PostGrant Proceedings with Parallel District Court Litigation (June 21, 2022), at 9. Here, the Petition is particularly strong and presents compelling evidence of unpatentability of the Challenged Claims. Specifically, the Petition explains how the prior art renders the Challenged Claims obvious – including by explicit teaching of the “device fingerprint” that purported to provide novelty during prosecution. The evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence. Thus, under the Interim Guidance, the Board should not deny institution.

Likewise, the Board’s decision in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (Dec. 1, 2020) (precedential as to § II.A) instructs that a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed in the District Court Litigation (§VIII.B). *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the earliest scheduled trial date has been set for October 20, 2025. Further, a Final Written Decision in this matter is expected in or around July, 2026. Because much can change in trial schedules, the current trial date does not support denial. *Dish Network v. Broadband iTV*, IPR2020-01280, Paper 17 at 16 (PTAB Feb. 4, 2021) (“We cannot ignore the fact that the currently scheduled trial date is more than nine months away and much can change during this time”).

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. The parties will not begin claim construction briefing until February 28, 2025. EX-1008, at 6. The *Markman* hearing is not until April 30, 2025. EX-1008, at 6. Fact discovery closes in May 9, 2025, and expert discovery closes in July 3, 2025. EX-1008, at 5; see *PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (little investment

in the parallel proceeding where claim construction hearing had not yet been held and discovery was not complete).

Under factor 4, there will not be any overlap in the issues raised in the IPR and in the co-pending litigation. If the Board institutes IPR, Petitioners stipulate to not raising in the Related litigations any grounds that include the same primary reference (Miller) used herein. Thus, Miller will be adjudicated against the '009 patent claims in one forum: the PTAB. Furthermore, although Petitioners challenge here all claims asserted in the co-pending litigation, PO has asserted 70 claims from 3 patents in Related Litigations (Ex-1016 at 3) – an amount that far exceeds the number of claims that the district court will allow at trial. *See <https://txed.uscourts.gov/?q=model-order-focusing-patent-claims-and-prior-art-reduce-costs>*. (Model Order limiting patentees to a “Final Election of Asserted Claims, which shall identify no more than five asserted claims per patent from among the ten previously identified claims and no more than a total of 16 claims”). Given that the PO will likely be limited to only five claims from the '009 Patent (at most), it is highly unlikely the district court will be addressing the validity of all of the claims challenged in this Petition.

Under factor 5, while Petitioners are defendants in District Court, nothing within *Fintiv* suggests that the same parties between the proceedings weighs in favor of discretionary denial. *See HP Inc. v. Slingshot Printing LLC*, IPR2020-01084,

Paper 13 at 9 (Jan. 14, 2021) (having the “same parties as parallel proceeding” makes factor 5 “neutral”).

Under factor 6, other circumstances weigh in favor of institution. Here, the Petition sets forth compelling merits of invalidity. Miller teaches the same architecture and the same functionality to achieve the same result of device verification as claimed in the '009 Patent. As discussed *supra*, the Examiner found most of the features in the prior art, but was likely not aware of the prior art identified in this Petition, which discloses or suggests precisely what the Examiner found lacking in the prior art. The Examiner would not have allowed the application over the prior art relied upon herein.

When viewed holistically, the timing of the present Petition is reasonable, there has been relatively limited investment in the EDTX litigation, and there is likely to be minimal overlap between the present IPR and the parallel litigation. Further, coupling these *Fintiv* considerations with compelling evidence of unpatentability presented in the Petition, the efficiency and integrity of the IPR process is best served by instituting review.

IX. MANDATORY NOTICES UNDER 37 C.F.R. §42.8

A. Real Parties-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioners are AT&T Services Inc., Cellco Partnership D/B/A Verizon Wireless, and Nokia Of America Corporation and are the real parties-in-interest.

Furthermore, Petitioners identify Microsoft Corporation, AT&T Mobility II LLC, AT&T Enterprises, LLC f/k/a AT&T Corp., AT&T Mobility LLC, Verizon Business Network Services LLC f/k/a Verizon Business Network Services, Inc., TracFone Wireless, Inc. and Verizon Corporate Services Group Inc. as a real-party-in-interest.⁴

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '009 Patent is asserted against Petitioners in *RightQuestion, LLC v. Cellco, Verizon Business Network Services LLC et al.*, No. 2:24-cv-00091 (E.D.

⁴ Out of an abundance of caution, Petitioners identify all current defendants in the below identified cases as potential real parties in interest only for the purpose of this proceeding and only to the extent that Patent Owner contends that these separate legal entities should be named real parties in interest in this IPR. Petitioners do so to avoid the potential expenditure of resources to resolve such a challenge. Petitioners also acknowledge that each petitioner has a number of affiliates. No unnamed entity is funding, controlling, or otherwise has an opportunity to control or direct this Petition or Petitioners' participation in any resulting IPR. Petitioners are also not aware of any affiliate that would be barred from filing this Petition under 35 U.S.C. § 315(e).

Tex.) filed February 9, 2024 and *RightQuestion, LLC v. AT&T Inc. et al*, 2:24-cv-00094 (E.D. Tex.) filed February 12, 2024.

To Petitioners' knowledge, as of the date of this filing, the '009 Patent was not involved in any additional cases that may be affected by a decision in this proceeding.

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

LEAD COUNSEL	BACK-UP COUNSEL
Kevin Anderson Reg. No. 43,471 KPAnderson@duanemorris.com DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20004 P: (202) 776-5213 F: (202) 776-7801	Glenn D. Richeson Reg. No. 73,780 GDRicheson@duanemorris.com DUANE MORRIS LLP 1075 Peachtree Street NE, Suite 1700 Atlanta, GA 30309-3929 P: (404) 253-6998 F: (404) 759-2703
	Brian H. Pandya Reg. No. 60,991 BHPandya@duanemorris.com DUANE MORRIS LLP 901 New York Avenue, NW, Ste. 700 East Washington, D.C. 20004 P: (202) 776-7807 F: (202) 776-7801

D. Service Information Under 37 C.F.R. § 42.8(b)(4)

Service via hand-delivery may be made at the postal mailing address of either lead or back-up counsel. Petitioners consent to service by e-mail at the addresses listed above.

X. CONCLUSION

Petitioners request the Board institute IPR and cancel all Challenged Claims.

Respectfully submitted,

/Kevin P. Anderson/

Kevin P. Anderson, USPTO Reg. No. 43,471
901 New York Avenue, N.W.

Suite 700 East

Washington, D.C. 20001

P: (202) 776-7800

F: (202) 776-7801

kpanderson@duanemorris.com

ATTORNEY FOR PETITIONERS

February 7, 2025

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 42.6(e), 42.8(b)(4) and 42.105, the undersigned certifies that on the 7th of February, 2025, a complete and entire copy of this Petition for *Inter Partes* Review of U.S. Patent No. 10,674,009 and all supporting exhibits were served by electronic means by agreement with Patent Owner to:

34060 - MICHAEL N. HAYNES
P.O. Box 460
RUCKERSVILLE, VA 22968
UNITED STATES

Service copies are also being sent via email to litigation counsel of record:

Robert F. Kramer
CA Bar No. 181706 (Admitted E.D. Texas)
rkramer@krameralberti.com
David Alberti
CA Bar No. 220265 (Admitted E.D. Texas)
dalberti@krameralberti.com
Sal Lim
CA Bar No. 211836 (Admitted E.D. Texas)
slim@krameralberti.com
Russell S. Tonkovich
CA Bar No. 233280 (Admitted E.D. Texas)
rtonkovich@krameralberti.com
Robert Mattson (pro hac vice)
Virginia Bar No. 43568
rmattson@krameralberti.com
Michele Woodruff Lyons
CA Bar No. 234891 (pro hac vice)
mlyons@krameralberti.com
Jeremiah A. Armstrong
CA Bar No. 253705 (pro hac vice)
jarmstrong@krameralberti.com
KRAMER ALBERTI LIM

& TONKOVICH LLP
577 Airport Blvd., Suite 250
Burlingame, CA 94010
Telephone: (650) 825-4300
Facsimile: (650) 460-8443

Nicole Glauser
Texas State Bar No. 24050694
nglauser@krameralberti.com
KRAMER ALBERTI LIM
& TONKOVICH LLP
500 W 2nd Street, Suite 1900
Austin, Texas 78701
Telephone: (737) 256-7784
Facsimile: (650) 460-8443

Andrea Fair
andrea@wsfirm.com
Ward, Smith & Hill, PLLC
1507 Bill Owens Parkway
Longview, TX 75604
(903) 757-6400
(903) 757-2323

/Kevin P. Anderson/
Kevin P. Anderson, Reg. No. 43,471
901 New York Avenue, N.W.
Suite 700 East
Washington, D.C. 20001
P: (202) 776-7800
F: (202) 776-7801
kpanderson@duanemorris.com

ATTORNEY FOR PETITIONERS

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24 *et seq.*, the undersigned certifies that this document complies with the type-volume limitations. This document contains 12,737 words as calculated by the “Word Count” feature of Microsoft Word 2010, the word processing program used to create it.

Dated: February 7, 2025

By: Kevin P. Anderson
Kevin P. Anderson
Reg. No. 43,471
Duane Morris LLP
901 New York Avenue, N.W.,
Suite 700 East
Washington D.C., 20001
P: (202) 776-7800
F: (202) 776-7801
kpanderson@duanemorris.com