

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE**

PROVE IDENTITY, INC.

Plaintiff,

v.

KYXSTART, INC.

Defendant.

C.A. No. _____

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff Prove Identity, Inc. (“Plaintiff” or “Prove”), by and through its undersigned counsel, files this Complaint against Defendant KYXStart, Inc. (“Defendant” or “KYXStart”), and alleges as follows:

NATURE OF THE ACTION

1. In this case, Prove seeks redress from the blatant and willful patent infringement committed by several of its former employees—employees who were in positions of leadership and trust at the company. Those employees worked for years at Prove, were privy to Prove’s most proprietary technology, and surreptitiously made off with Prove’s inventions to build a direct competitor—KYXStart—on a corrupt foundation of patent infringement. Now, having avoided much of the cost, risk, and considerable time and effort Prove endured to conceive, develop, and perfect its products, KYXStart competes directly with Prove, forcing Prove to battle with its own innovations in the marketplace. For these reasons, Prove brings this action for patent infringement under the Patent Laws of the United States, 35 U.S.C. §§ 100 et seq., including 35 U.S.C. § 271, and for tortious interference with contract under Delaware state law.

2. Prove, formerly known as Payfone, Inc., is a leader and innovator in the field of digital identity verification and authentication. Legacy authentication methods cannot keep up with modern identity needs. Modern threats exploit every gap between sessions, signals, and user behavior. Recognizing this need, Prove developed innovative new technologies and identity verification and authentication architectures that bridge these gaps, and leverage characteristics about the user and their devices in the real world to confirm their digital identity. These Prove-invented technologies enable businesses to verify the identity of individuals in a fast, secure, and frictionless manner, helping to mitigate fraud while improving the consumer experience.

3. In recognition of Prove's many innovations, the U.S. Patent and Trademark Office issued the following United States Patents, among others: U.S. Patent Nos. 12,058,528 ("528 patent") and 12,200,816 ("816 patent") (collectively the "Asserted Patents" or "Patents-in-Suit").

4. KYXStart is and has been infringing the Asserted Patents with its identity verification products and services, including without limitation Person Verification (KYC), Business Verification (KYB), Payments Verification (KYP), Telco Intelligence, Fraud Intelligence, Ongoing AML Monitoring, and the software and hardware implementing these products and services, such as verification-related software modules, computer-readable instructions, processors, and servers,¹ and any instrumentalities identified and referenced in the attached claim charts not listed here (collectively, the "Accused Products").

5. Among the employees who left Prove to found KYXStart is Ravindra Bijlani, who is the former Senior Vice President, International & Global Alliances at Prove. Renata Lowenbraun, Prove's former Vice President—Legal, Privacy & Product, is now the General Counsel

¹ See, e.g., <https://www.kyxstart.com/> (presenting, among other things, information about software, software modules, and service architectures relating to digital authentication and identity verification); see also Exhibits C-D (infringement claim charts).

at KYXStart. More recently, KYXStart induced Michael Stearne to become its Head of Product, knowing he had worked at Prove as its Director of Product Management, and knowing he was contractually bound by a non-compete agreement with Prove. These former Prove employees have first-hand knowledge of Prove's innovations, including those covered by the claims in the Asserted Patents. Indeed, Mr. Stearne is a *named inventor* on those Patents. Instead of competing fairly with its own home-grown technology, KYXStart, through Mr. Stearne and others, has developed products and services that willfully and flagrantly infringe on Prove's patented technology.

6. Prove seeks, among other relief, damages adequate to compensate for KYXStart's infringement of the Asserted Patents, enhanced damages for willful infringement, injunctive relief, damages for tortious interference with contract, and attorneys' fees and costs.

PARTIES

7. Prove is a corporation organized under the laws of the State of Delaware, with a principal place of business at 245 Fifth Avenue, 20th Floor, New York, NY 10016.

8. On information and belief, KYXStart is a corporation organized under the laws of the State of Delaware, with a place of business located at 1055 Lillian Drive, Alpharetta, Georgia 30004. KYXStart has a registered agent to accept service of process within the State of Delaware located at United States Corporation Agents, Inc., 131 Continental Drive, Suite 305, Newark, Delaware 19713.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over the patent infringement claims in this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because they arise under the patent laws of the United States.

10. The Court has supplemental jurisdiction over the state law tortious interference with contract claim pursuant to 28 U.S.C. § 1367(a) because that claim is so related to the patent infringement claims within this Court's original jurisdiction that it forms part of the same case or controversy.

11. The Court has personal jurisdiction over KYXStart. KYXStart is subject to general personal jurisdiction because it is incorporated in the State of Delaware.

12. Venue is proper in this District under 28 U.S.C. § 1400(b). KYXStart resides in this District because it was and is incorporated under the laws of the State of Delaware.

PATENTS-IN-SUIT

A. The '528 Patent

13. The '528 patent, titled "Identity Network Representation of Communications Device Subscriber in a Digital Domain," was duly and legally issued on August 6, 2024, and names Prashant Janakrai Desai, David Louis Berra, Rodger R. Desai, Michael Bijelich, Jeffrey Robert Naujok, and Michael Stearne as the inventors. A true and correct copy of the '528 patent is attached as Exhibit A.

14. The '528 patent describes and claims, among other things, methods and apparatus comprising receiving, by an identity verifier computing device from a communications device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity; establishing, by the identity verifier computing device, a plurality of nodes of an identity network, wherein: the identity network exists in an electronic or digital domain, the identity network is associated with the real-world identity via a persistent identifier, each node in the plurality of nodes is associated with the persistent identifier via a set of links, and each link in the set of links includes a trustworthiness parameter; responsive to a first set of interactions

by a first aspect of a set of aspects with at least a first node of the plurality of nodes, updating, by the identity verifier computing device, a first trustworthiness parameter of a first link between a second node of the plurality of nodes and a second aspect of the set of aspects; and transmitting, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device, wherein the verification is based, at least in part, on the first link.

15. The '528 patent claims specific, unconventional technical solutions that were not well-understood, routine, or conventional in the art and that represent inventive concepts going well beyond any abstract idea. This includes, without limitation, the claimed identity-network architecture in which a plurality of nodes are associated with a persistent identifier via a set of links, each link carrying a trustworthiness parameter, and a cross-link trust-propagation mechanism that dynamically updates the trustworthiness parameter of one link in response to interactions occurring at a different node–aspect pair. The combined elements in the claims of the '528 patent recite a defined, graph-based identity-verification architecture that goes well beyond any abstract concept. The claimed combination of features improves the technical capabilities of computer systems for digital identity management—enabling an identity verifier computing device to synthesize real-world identity signals and digital-domain interaction data through a coordinated trust-propagation framework, and to condition the ultimate subscriber co-location verification on the dynamically computed state of a specific link, in a manner no prior system could accomplish.

16. Prove is the assignee of the entire right, title, and interest in the '528 patent.

B. The '816 Patent

17. The '816 patent, titled “Transmitting a Complement of User Parameters to a Communications Device,” was duly and legally issued on January 14, 2025, and names Jeffrey Robert

Naujok, Prashant Janakrai Desai, Michael Stearne, Rodger R. Desai, Ryan Alexander, and Kyle Price as the inventors. A true and correct copy of the '816 patent is attached as Exhibit B.

18. The '816 patent describes and claims, among other things, methods and apparatus comprising electronically verifying, via a particular authentication operation at a computing device, possession of a communications device by a subscriber of a communications network at least in part by: receiving, from the communications device, an authentication request that includes a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation, and determining that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window; receiving, at the computing device via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network; determining, at the computing device, an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII; and communicating, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network.

19. The '816 patent claims specific, unconventional technical solutions that were not well-understood, routine, or conventional in the art and that represent inventive concepts going well beyond any abstract idea. This includes, without limitation, the claimed multi-step authentication architecture employing a time-limited-type identifier that is unique to a particular authentication operation, passed between a computing device and a communications device to maintain a

persistent linkage across a plurality of steps of the authentication operation, and validated based on the number of times it has been included in authentication requests received within a recent time window. The combined elements in the claims of the '816 patent recite a defined, session-integrity protocol that goes well beyond any abstract concept. The claimed combination of features improves the technical capabilities of computer systems for secure, multi-step device authentication—enabling a computing device to detect and prevent third-party interception or replay attacks during an authentication session by binding the session to a unique, ephemeral identifier and monitoring its request frequency in a manner no prior system accomplished.

20. Prove is the assignee of the entire right, title, and interest in the '816 patent.

KNOWLEDGE AND WILLFULNESS

21. Ravindra Bijlani was a senior employee at Prove, having joined the company on or about October 30, 2017, as Vice President, Strategic Partnerships. He departed Prove in or about June 2022.

22. As a condition of his employment, Mr. Bijlani was required to execute, and did execute, a Proprietary Information and Inventions Agreement (the “PIIA”) on October 14, 2017, and had, during his tenure at Prove, access to Prove’s Proprietary Information, including information relating to the innovations that became the subject of the Asserted Patents.

23. Mr. Bijlani went on to co-found KYXStart and is its CEO. The association of Mr. Bijlani with KYXStart—who had, through his tenure, knowledge of the inventions that became the subject of the Asserted Patents—further demonstrates that KYXStart had actual knowledge of the Asserted Patents, the scope of the claimed inventions, and the infringing nature of the Accused Products.

24. Renata Lowenbraun was a senior employee at Prove, having joined the company on or about July 29, 2019, as Vice President—Legal, Privacy & Product. She departed Prove in or about March 2022.

25. During her tenure at Prove, Ms. Lowenbraun oversaw Prove’s patent prosecutions as part of her duties and had access to Prove’s Proprietary Information, including information relating to the innovations that became the subject of the Asserted Patents.

26. Ms. Lowenbraun joined KYXStart as a legal advisor in January 2025 and has since then been its General Counsel.² The association of Ms. Lowenbraun with KYXStart—who had, through her tenure, knowledge of the inventions that became the subject of the Asserted Patents—further demonstrates that KYXStart had actual knowledge of the Asserted Patents, the scope of the claimed inventions, and the infringing nature of the Accused Products.

27. Michael Stearne was a significant and senior employee at Prove during his tenure with the company. He joined the company as a Sales Engineer in May 2017 and was promoted to Global Product Manager in April 2019 and Director of Product Management in November 2022. Michael Stearne left Prove in October 2024 and joined KYXStart as a consultant, holding the role of KYXStart’s Head of Product since January 2025.³

28. During his tenure at Prove, Mr. Stearne gained extensive knowledge of Prove’s proprietary identity verification and digital authentication technology, including the technical and operational aspects of the products and systems Prove developed and provided.

² See Renata Lowenbraun (@renatalowenbraun), LINKEDIN, <https://www.linkedin.com/in/re-natalowenbraun> [https://perma.cc/7CFD-JYSK] (last visited Sept. 28, 2026).

³ See Michael Stearne (@mstearne), LINKEDIN, <https://www.linkedin.com/in/mstearne/> [https://perma.cc/X7G6-6QHD] (last visited Sept. 28, 2026).

29. Mr. Stearne is a named inventor on both Asserted Patents and, accordingly, had direct, detailed, and first-hand knowledge of the patented inventions, the technology claimed in the Asserted Patents, and the Asserted Patents' prosecution history.

30. By virtue of his inventorship and his access to Prove's proprietary information, Mr. Stearne possessed particularized knowledge of the scope and substance of the Asserted Patents, including the technical innovations embodied therein.

31. On information and belief, KYXStart knowingly and intentionally recruited and engaged Mr. Stearne as a consultant by January 2025, with knowledge of his role at Prove developing the patented technology and his inventorship of both Asserted Patents.

32. KYXStart's specific and selective recruitment and engagement of Mr. Stearne was designed to obtain a competitive advantage by accessing his knowledge of Prove's innovations, including the inventions claimed in the Asserted Patents.

33. Through its recruitment and engagement of Mr. Stearne as a consultant, KYXStart obtained actual knowledge of the Asserted Patents and the scope of the claimed inventions.

34. On March 5, 2026, Prove sent KYXStart a letter providing notice of the Asserted Patents and informing KYXStart of its belief that KYXStart's products and services infringe the Asserted Patents.

35. On April 2, 2026, KYXStart, through its outside counsel, Blank Rome LLP, responded to Prove's notice letter. In its response, KYXStart expressly identified both U.S. Patent No. 12,058,528 and U.S. Patent No. 12,200,816 by number and purported to address the scope of each patent's claims, including with non-infringement arguments that were based on erroneous

constructions of the claims of the Asserted Patents and misstatements of facts concerning KYXStart's infringing products. KYXStart had actual knowledge of the Asserted Patents and their claims, and KYXStart's infringement at least as of its receipt of Prove's notice letter.

36. Despite its knowledge of the Asserted Patents, their claims, and KYXStart's infringement of at least one of those claims since at least its hiring of former Prove employees and its receipt of Prove's notice letter, KYXStart has continued to make, use, sell, and offer to sell the Accused Products without authority or license from Prove. KYXStart's continued infringement following receipt of Prove's notice letter was and is willful, deliberate, and in conscious disregard of Prove's patent rights.

COUNT I

(Infringement of the '528 Patent)

37. Prove realleges and incorporates the allegations of the preceding paragraphs of this complaint as though fully stated herein.

38. KYXStart has directly infringed and continues to infringe, literally and/or under the doctrine of equivalents, the '528 patent by making, using, selling, and/or offering for sale in the United States the Accused Products, which in operation meet the limitations of the patented methods in the '528 patent, in violation of 35 U.S.C. § 271. Exemplary evidence and an exemplary chart mapping a claim of the '528 patent to the Accused Products and demonstrating KYXStart's infringement can be found in Exhibit C. Prove anticipates identifying additional asserted claims in accordance with the case schedule and its discovery obligations.

39. KYXStart also has been and is inducing infringement of the '528 patent by actively encouraging its customers and licensees to directly infringe the patented methods claimed therein. On information and belief, KYXStart's customers and licensees—including Tacilent.ai and Trident3—directly infringe the '528 patent by implementing and using the Accused Products in a

manner that practices the limitations of the patented methods.⁴ As pleaded above, KYXStart was aware of the Asserted Patents, and knew or was willfully blind to the fact that its customers' and licensees' use of the Accused Products would constitute infringement. KYXStart has taken purposeful, culpable, and affirmative steps beyond ordinary acts incident to product distribution designed to bring about that infringement as its desired result. These purposeful, culpable, and affirmative steps include, but are not limited to, actively partnering with its customers to create and deploy specific infringing implementations of the Accused Products, providing technical support and consulting services to instruct customers to use the Accused Products in an infringing manner, and publicizing those infringing deployments through its own website and press releases in a manner designed to stimulate additional customers and licensees to adopt the same infringing use. These aforementioned acts have no obvious alternative explanation other than to bring about the use of the Accused Products in a manner that infringes the '528 patent. *See* footnote 6.

40. In the alternative and additionally, for at least the reasons pleaded above in Paragraphs 21–36, KYXStart subjectively believed there was a high probability that its customers directly infringed the '528 patent but nevertheless deliberately took steps to avoid learning that fact, in other words, willfully blinded itself to the infringing nature of the direct infringer's acts.

41. For at least these reasons, KYXStart's infringement has been, and continues to be, knowing, intentional, and willful.

⁴ *See, e.g.*, Tacilent.ai Partners with KYXStart to Launch Real-Time “Know Your Entity” and “Know Your Vendor” Risk Intelligence, EZ NEWSWIRE, *available at* <https://www.eznews-wire.com/newsroom/tacilent-partners-with-kyxstart-to-launch-real-time-know-your-entity-and-know-your-vendor-risk-intelligence> (last visited Sept. 18, 2026); KYXSTART and Trident3 Announce Strategic Partnership to Integrate Digital Identity at the Infrastructure Layer, Building Trust in DeFi to Drive Mass Adoption, MEDIUM, *available at* <https://medium.com/@trident3/for-immediate-release-89acdc78924e> (last visited Sept. 18, 2026); Trust at Every Trust Point, <https://www.kyxstart.com/company> (last visited Sept. 22, 2026) (listing companies that appears to be KYXStart's customers, including Instarails, Everyware, and N2N).

42. KYXStart's acts of infringement have caused and will continue to cause Prove damages for which Prove is entitled to compensation—which shall in no event be less than a reasonable royalty—and an increase in the damages award to Prove of up to three times that amount, pursuant to 35 U.S.C. § 284.

43. This case is exceptional and, therefore, Prove is entitled to an award of attorneys' fees pursuant to 35 U.S.C. § 285.

COUNT II

(Infringement of the '816 Patent)

44. Prove realleges and incorporates the allegations of the preceding paragraphs of this complaint as though fully stated herein.

45. KYXStart has directly infringed and continues to infringe, literally and/or under the doctrine of equivalents, the '816 patent by making, using, selling, and/or offering for sale in the United States the Accused Products, which in operation meet the limitations of the patented methods in the '816 patent, in violation of 35 U.S.C. § 271. Exemplary evidence and an exemplary chart mapping a claim of the '816 patent to the Accused Products and demonstrating KYXStart's infringement can be found in Exhibit D. Prove anticipates identifying additional asserted claims in accordance with the case schedule and its discovery obligations.

46. KYXStart also has been and is inducing infringement of the '816 patent by actively encouraging its customers and licensees to directly infringe the patented methods claimed therein. On information and belief, KYXStart's customers and licensees—including Tacilent.ai and Trident3—directly infringe the '816 patent by implementing and using the Accused Products in a

manner that practices the limitations of the patented methods.⁵ As pleaded above, KYXStart was aware of the Asserted Patents, and knew or was willfully blind to the fact that its customers' and licensees' use of the Accused Products would constitute infringement. KYXStart has taken purposeful, culpable, and affirmative steps beyond ordinary acts incident to product distribution designed to bring about that infringement as its desired result. These purposeful, culpable, and affirmative steps include, but are not limited to, actively partnering with its customers to create and deploy specific infringing implementations of the Accused Products, providing technical support and consulting services to instruct customers to use the Accused Products in an infringing manner, and publicizing those infringing deployments through its own website and press releases in a manner designed to stimulate additional customers and licensees to adopt the same infringing use. These aforementioned acts have no obvious alternative explanation other than to bring about the use of the Accused Products in a manner that infringes the '816 patent. *See* footnote 7.

47. In the alternative and additionally, for at least the reasons pleaded above in Paragraphs 21–36, KYXStart subjectively believed there was a high probability that its customers directly infringed the '816 patent but nevertheless deliberately took steps to avoid learning that fact, in other words, willfully blinded itself to the infringing nature of the direct infringer's acts.

48. For at least these reasons, KYXStart's infringement has been, and continues to be, knowing, intentional, and willful.

⁵ *See, e.g.*, Tacilent.ai Partners with KYXStart to Launch Real-Time “Know Your Entity” and “Know Your Vendor” Risk Intelligence, EZ NEWSWIRE, *available at* <https://www.eznews-wire.com/newsroom/tacilent-partners-with-kyxstart-to-launch-real-time-know-your-entity-and-know-your-vendor-risk-intelligence> (last visited Sept. 18, 2026); KYXSTART and Trident3 Announce Strategic Partnership to Integrate Digital Identity at the Infrastructure Layer, Building Trust in DeFi to Drive Mass Adoption, MEDIUM, *available at* <https://medium.com/@trident3/for-immediate-release-89acdc78924e> (last visited Sept. 18, 2026); Trust at Every Trust Point, <https://www.kyxstart.com/company> (last visited Sept. 22, 2026) (listing companies that appears to be KYXStart's customers, including Instarails, Everyware, and N2N).

49. KYXStart's acts of infringing the '816 patent have caused and will continue to cause Prove damages for which Prove is entitled to compensation—which shall in no event be less than a reasonable royalty—and an increase in the damages award to Prove of up to three times that amount, pursuant to 35 U.S.C. § 284.

50. This case is exceptional and, therefore, Prove is entitled to an award of attorneys' fees pursuant to 35 U.S.C. § 285.

COUNT III

(Tortious Interference with Contract)

51. Prove realleges and incorporates the allegations of the preceding paragraphs of this complaint as though fully stated herein.

52. On May 10, 2017, Prove extended an offer of employment to Michael Stearne. Mr. Stearne executed the offer letter on May 11, 2017.

53. As a condition of his employment, Mr. Stearne was required to execute, and did execute, a PIIA on May 11, 2017.

54. The PIIA contained post-employment restrictive covenants. Specifically, Section 4(d) of the PIIA provided that, for a period of one (1) year immediately following termination of Mr. Stearne's employment (for any or no reason, whether voluntary or involuntary), he would not directly or indirectly: (i) Cause any person to leave their employment with Prove; (ii) Solicit any Business Partner; or (iii) act in "Any Capacity" in or with respect to any "Competing Business" located within the State of New York, the rest of the United States, or anywhere else in the world.

55. The PIIA further required Mr. Stearne to hold in confidence and not disclose or use any Proprietary Information of Prove, including all business, technical, and financial information, and information relating to Prove's employees, Affiliates, and Business Partners.

56. Under Section 6 of the PIIA, Mr. Stearne's obligations under Sections 2, 3, and 4 of the PIIA expressly survived the termination of his employment, regardless of the reason for termination and whether voluntary or involuntary.

57. Prior to Mr. Stearne's departure from Prove in or about October 2024, Mr. Stearne executed a separation agreement (the "Separation Agreement") that expressly incorporated and required him to continue to comply with the obligations set forth in the PIIA, including, without limitation, the one-year post-employment restrictive covenant in Section 4(d) (the "Restrictive Covenant").

58. The offer letter, the PIIA, and the Separation Agreement (collectively, the "Stearne Agreements") constituted valid and enforceable contracts between Prove and Mr. Stearne that were supported by adequate consideration and were in full force and effect at all times relevant hereto.

59. On information and belief, KYXStart had knowledge of the existence of the Stearne Agreements, including the Restrictive Covenant, at the time it recruited and hired Mr. Stearne, or, at a minimum, knew facts from which the existence of such contractual obligations could reasonably be inferred.

60. On information and belief, KYXStart knew or should have known that Mr. Stearne was subject to post-employment restrictive covenants because: (a) it is standard practice in the identity verification and digital authentication industry for companies to require employees to execute proprietary information and non-compete agreements; (b) KYXStart itself requires its employees to execute similar agreements; (c) Mr. Stearne's senior position at Prove, a direct competitor of KYXStart in the identity verification space, made it readily foreseeable that Mr. Stearne was bound by such agreements; and (d) KYXStart's senior employees and executives, including Mr. Bijlani, were ex-Prove employees who also executed and had knowledge of the same PIIA,

and Ms. Lowenbraun as Prove's former Vice President, Legal, Privacy & Product should be aware of Prove's practice of signing a PIIA with employees containing post-employment restrictive covenants. Further, on information and belief, Mr. Stearne told KYXStart about his post-employment restrictive covenants.

61. On information and belief, KYXStart learned of the Restrictive Covenant, and proceeded to recruit and engage Mr. Stearne in deliberate disregard thereof, or alternatively, KYXStart failed to make any reasonable inquiry into Mr. Stearne's contractual obligations to Prove before recruiting and engaging him.

62. Mr. Stearne departed Prove in October 2024. On information and belief, Mr. Stearne joined KYXStart in January 2025 as a consultant—within the one-year restricted period under the Restrictive Covenant—in breach of his obligations under the Stearne Agreements.

63. On information and belief, KYXStart specifically and selectively recruited Mr. Stearne, a key employee of Prove with extensive knowledge of Prove's proprietary identity verification technology and the Asserted Patents, for the purpose of obtaining a competitive advantage.

64. KYXStart's recruitment and engagement of Mr. Stearne was a significant factor in causing Mr. Stearne to breach the Restrictive Covenant and his confidentiality obligations under the PIIA and the Stearne Agreements.

65. On information and belief, KYXStart actively pursued Mr. Stearne, including offers of engagement or compensation, and sought to bring about Mr. Stearne to breach his contractual obligations to Prove under the Stearne Agreements, including but not limited to the obligations not to compete with Prove.

66. On information and belief, KYXStart's intentional recruitment and engagement of Mr. Stearne as a consultant was without justification or privilege. KYXStart had no legitimate

business reason to recruit an employee it knew or should have known was bound by enforceable restrictive covenants prohibiting him from working for a competitor of Prove during the agreed period.

67. As a direct and proximate result of KYXStart's knowing and intentional conduct of engaging Mr. Stearne, Prove has suffered and continues to suffer injury, including but not limited to: (a) loss of the benefit of the bargain for which Prove contracted under the Stearne Agreements; (b) competitive harm resulting from Mr. Stearne's engagement by a direct competitor before expiration of the restricted period; (c) the risk of disclosure and misappropriation of Prove's Proprietary Information, including trade secrets, business strategies, customer information, and technical know-how relating to Prove's identity verification technology; and (d) harm to Prove's goodwill, customer relationships, and competitive position in the market.

68. As a result of KYXStart's intentional and unjustified interference in Mr. Stearne's performance of his agreements, Prove has suffered damages, including but not limited to loss of the benefits for which it bargained in the Stearne Agreements, harm to its competitive position and goodwill, unjust enrichment of KYXStart, and economic loss, in an amount to be determined at trial.

69. KYXStart's conduct was intentional, willful, wanton, and in reckless disregard of Prove's rights, warranting an award of punitive damages in an amount to be determined at trial.

70. KYXStart's tortious interference with the Stearne Agreements was part of a unified scheme of unfair competition: KYXStart infringed the Asserted Patents with the Accused Products and poached Prove's key personnel—including a named inventor of those patents—to further facilitate that infringing activity. Because Prove's tortious interference claim arises from the same conduct, actors, and evidence as its willful patent infringement claims, the claims share a common

nucleus of operative facts and form part of the same case or controversy, warranting the exercise of supplemental jurisdiction under 28 U.S.C. § 1367(a).

JURY DEMAND

Prove demands a jury trial on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Prove respectfully requests that the Court find in its favor and against KYXStart, and grant Prove the following relief:

- a. A judgment that KYXStart has infringed and is infringing, directly and indirectly, the '528 patent and '816 patent;
- b. A judgment that KYXStart must account for and pay damages adequate to compensate Prove for KYXStart's infringement of one or more claims of the Asserted Patents, including for post-trial infringing acts, pursuant to 35 U.S.C. § 284, which shall in no event be less than a reasonable royalty;
- c. A judgment that KYXStart has willfully infringed the '528 patent and '816 patent, and an increase in the damages award to Prove of up to three times the amount assessed, pursuant to 35 U.S.C. § 284;
- d. A declaration that this case is exceptional and an award of reasonable attorneys' fees in accordance with 35 U.S.C. § 285;
- e. A judgment that KYXStart has tortiously interfered with the Stearne Agreements;
- f. An award of compensatory damages for KYXStart's tortious interference with the Stearne Agreements, including loss of the benefit of Prove's bargain, competitive harm, and unjust enrichment;

- g. An award of punitive damages for KYXStart's willful and bad-faith tortious interference with the Stearne Agreements;
- h. Injunctive relief to prevent further misuse of Prove's Proprietary Information obtained through KYXStart's tortious interference;
- i. Pre-judgment and post-judgment interest on damages;
- j. Costs of this action; and
- k. All other and further relief as this Court deems just and proper.

Dated: October 14, 2026

OF COUNSEL:

Douglas E. Lumish
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
201 Redwood Shores Parkway
Redwood Shores, California 94065
Telephone: (650) 802-3190
doug.lumish@weil.com

Joseph H. Lee
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
1999 Avenue of the Stars
Los Angeles, California 90067
Telephone: (213) 667-5190
joseph.lee@weil.com

Bryce Bing Liu
(*pro hac vice* forthcoming)
WEIL, GOTSHAL & MANGES LLP
2001 M Street NW, Suite 600
Washington, DC 20036
Telephone: (202) 682-7000
bryce.liu@weil.com

/s/ Travis S. Hunter
Travis S. Hunter (#5350)
Alexandra Ewing (#6407)
RICHARDS, LAYTON
& FINGER, P.A.
920 North King Street
Wilmington, Delaware 19801
(302) 651-7700
hunter@rlf.com
ewing@rlf.com

Attorneys for Plaintiff Prove Identity, Inc.

EXHIBIT A



US012058528B2

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

(10) **Patent No.:** **US 12,058,528 B2**
(45) **Date of Patent:** **Aug. 6, 2024**

(54) **IDENTITY NETWORK REPRESENTATION
OF COMMUNICATIONS DEVICE
SUBSCRIBER IN A DIGITAL DOMAIN**

(56) **References Cited**

U.S. PATENT DOCUMENTS

(71) Applicant: **PROVE IDENTITY, INC.**, New York,
NY (US)

5,727,163 A 3/1998 Bezos
5,874,918 A 2/1999 Czarnecki
(Continued)

(72) Inventors: **Prashant Janakrai Desai**, New York,
NY (US); **David Louis Berra**, Arvada,
CO (US); **Rodger R. Desai**, New York,
NM (US); **Michael Bijelich**, New York,
NY (US); **Jeffrey Robert Naujok**,
Colorado Springs, CA (US); **Michael
Stearne**, Bellmawr, NJ (US)

FOREIGN PATENT DOCUMENTS

EP 1936528 3/2014
JP H11338933 12/1999
(Continued)

OTHER PUBLICATIONS

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

U.S. Appl. No. 16/730,878: Final Office Action dated Mar. 28, 2023,
22 pages, Doc 1889.

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 109 days.

(Continued)

Primary Examiner — Dao Q Ho

(74) *Attorney, Agent, or Firm* — Husch Blackwell LLP;
Bryan D. Stewart; Matthew Francis

(21) Appl. No.: **17/565,427**

(22) Filed: **Dec. 29, 2021**

(65) **Prior Publication Data**

US 2022/0210657 A1 Jun. 30, 2022

Related U.S. Application Data

(60) Provisional application No. 63/133,127, filed on Dec.
31, 2020.

(51) **Int. Cl.**
H04W 12/72 (2021.01)
H04W 12/12 (2021.01)

(52) **U.S. Cl.**
CPC **H04W 12/72** (2021.01); **H04W 12/12**
(2013.01)

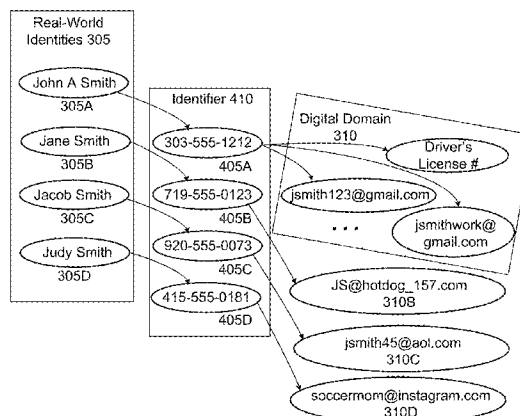
(58) **Field of Classification Search**
CPC H04W 12/72; H04W 76/12
See application file for complete search history.

(57) **ABSTRACT**

Briefly, example methods, apparatuses, and/or articles of
manufacture are disclosed that may be implemented to
represent an identity network corresponding to a communi-
cations device subscriber in an electronic or digital domain.
The method may include transmitting a message to a com-
munications device. Responsive to the transmitted message,
an authenticator may receive a signal to verify that a
subscriber having a real-world identity is co-located with the
communications device. The method may continue with
establishing, in an electronic or digital domain, two or more
nodes of an identity network corresponding to aspects of the
real-world identity of the subscriber, the identity network
being attached to the real-world identity via a persistent
identifier, and the two or more nodes of the identity network
being linked via one or more relationships.

25 Claims, 10 Drawing Sheets

400



US 12,058,528 B2

Page 2

(56)	References Cited						
	U.S. PATENT DOCUMENTS						
	5,930,474	A	7/1999	Dunworth		2007/0094150	A1 4/2007 Yuen
	6,012,144	A	1/2000	Pickett		2007/0157304	A1 7/2007 Logan
	6,130,937	A	10/2000	Fotta		2007/0167171	A1 7/2007 Bishop
	6,134,316	A *	10/2000	Kallioniemi	 H04W 8/28	2007/0169174	A1 7/2007 Critten
					379/211.02	2007/0174904	A1 7/2007 Park
	6,151,631	A	11/2000	Ansell		2007/0186095	A1 8/2007 Ganesan
	6,249,252	B1	6/2001	Dupray		2007/0198437	A1 8/2007 Eisner
	6,684,250	B2	1/2004	Anderson		2007/0250920	A1 10/2007 Lindsay
	6,748,367	B1	6/2004	Lee		2007/0279227	A1 12/2007 Juels
	6,757,740	B1	6/2004	Parekh		2007/0283273	A1 12/2007 Woods
	6,769,030	B1	7/2004	Bournas		2007/0292349	A1 12/2007 Griswold
	6,947,978	B2	9/2005	Huffman		2007/0300070	A1 12/2007 Shen-Orr
	6,968,194	B2	11/2005	Aljadeff		2008/0028447	A1 1/2008 O'Malley
	7,100,204	B1	8/2006	Myllymaki		2008/0034216	A1 2/2008 Law
	7,194,354	B1	3/2007	Oran		2008/0037536	A1 2/2008 Padmanabhan
	7,587,368	B2	9/2009	Felsher		2008/0052180	A1 2/2008 Lawhorn
	7,657,522	B1	2/2010	Puzicha		2008/0109657	A1 5/2008 Beiai
	8,136,148	B1	3/2012	Chayanam		2008/0120707	A1 5/2008 Ramia
	8,238,532	B1	8/2012	Cox		2008/0137554	A1 6/2008 Nandhra
	8,341,236	B1	12/2012	Ganesan		2008/0167106	A1 7/2008 Lutnick
	8,364,758	B2	1/2013	Hydrie		2008/0172730	A1 7/2008 Sandhu
	8,438,382	B2	5/2013	Ferg		2008/0182598	A1 7/2008 Bowman
	8,490,168	B1	7/2013	Holloway		2008/0214153	A1 9/2008 Ramer
	8,549,601	B2	10/2013	Ganesan		2008/0254765	A1 10/2008 Eilaz
	8,589,459	B1	11/2013	Ganesan		2008/0313719	A1 12/2008 Kaliski, Jr.
	8,589,532	B2	11/2013	Tenny		2009/0083430	A1 3/2009 Edge
	8,789,153	B2	7/2014	Ganesan		2009/0037983	A1 4/2009 Chiruvolu
	8,806,592	B2	8/2014	Ganesan		2009/0093300	A1 4/2009 Lutnick
	9,325,702	B2	4/2016	Ganesan		2009/0106138	A1 4/2009 Smith
	9,349,014	B1	5/2016	Hubing et al.		2009/0119754	A1 5/2009 Schubert
	9,819,680	B2	11/2017	Grigg		2009/0119776	A1 5/2009 Painitkar
	9,870,464	B1	1/2018	Kane-Parry et al.		2009/0132813	A1 5/2009 Schibuk
	10,284,549	B2	5/2019	Ganesan		2009/0222581	A1 9/2009 Josefsberg
	10,454,897	B1	10/2019	Rajanna		2009/0232515	A1 9/2009 Marien
	10,552,823	B1	2/2020	Woodward		2009/0235339	A1 9/2009 Mennes
	10,581,834	B2	3/2020	Ganesan		2009/0249076	A1 10/2009 Reed
	10,587,683	B1	3/2020	Ganesan		2009/0249077	A1 10/2009 Gargaro
	10,686,781	B1	6/2020	Kaditz et al.		2009/0254572	A1 10/2009 Redlich
	10,771,624	B1	9/2020	Penar		2009/0259588	A1 10/2009 Lindsay
	10,824,702	B1	11/2020	Shahidzadeh et al.		2009/0259848	A1 10/2009 Williams
	2002/0049644	A1	4/2002	Kargman		2009/0265768	A1 10/2009 Labaton
	2002/0069037	A1	6/2002	Hendrickson		2009/0265776	A1 10/2009 Baentsch
	2002/0095507	A1	7/2002	Jerdonek		2009/0288159	A1 11/2009 Husemann
	2003/0028451	A1	2/2003	Ananian		2009/0307767	A1 12/2009 Semba
	2003/0046022	A1	3/2003	Silverman		2009/0328168	A1 12/2009 Lee
	2003/0092421	A1	5/2003	Dolwin		2009/0328173	A1 12/2009 Jakobson et al.
	2003/0093341	A1	5/2003	Millard		2010/0017860	A1 1/2010 Ishida
	2003/0138084	A1	7/2003	Lynam		2010/0024022	A1 1/2010 Wells
	2003/0157963	A1	8/2003	Collot		2010/0041391	A1 2/2010 Spivey
	2004/0030924	A1	2/2004	Griswold		2010/0080369	A1 4/2010 Hurst et al.
	2004/0030934	A1	2/2004	Mizoguchi		2010/0128291	A1 5/2010 Vendrow
	2004/0210536	A1 *	10/2004	Gudelj	 G07F 19/206	2010/0131670	A1 5/2010 Ishii
					705/64	2010/0153540	A1 6/2010 Li
	2004/0225878	A1	11/2004	Costa-Requena		2010/0180328	A1 7/2010 Moas
	2004/0242238	A1	12/2004	Wang		2010/0235897	A1 9/2010 Mason
	2005/0018611	A1	1/2005	Chan		2010/0242104	A1 9/2010 Wankmueller
	2005/0071417	A1	3/2005	Taylor		2010/0262834	A1 10/2010 Freeman
	2005/0135242	A1	6/2005	Larsen		2010/0268831	A1 10/2010 Scott
	2005/0172229	A1	8/2005	Reno		2010/0312703	A1 12/2010 Kulpati et al.
	2005/0254653	A1	11/2005	Potashnik		2010/0325427	A1 12/2010 Ekberg
	2006/0168259	A1	7/2006	Spilotro		2010/0329125	A1 12/2010 Roberts
	2006/0168663	A1	7/2006	Viljoen		2011/0047372	A1 2/2011 Ganesan
	2006/0206709	A1	9/2006	Labrou		2011/0072499	A1 3/2011 Lin
	2006/0229996	A1	10/2006	Keithley		2011/0086616	A1 4/2011 Brand
	2006/0235795	A1	10/2006	Johnson		2011/0151843	A1 6/2011 Deuel
	2006/0239199	A1	10/2006	Blair		2011/0153496	A1 6/2011 Royyuru
	2006/0282662	A1	12/2006	Whitcomb		2011/0159848	A1 6/2011 Pei
	2007/0011312	A1	1/2007	Nakamura		2011/0161989	A1 6/2011 Russo
	2007/0011724	A1	1/2007	Gonzalez		2011/0191823	A1 8/2011 Huibers
	2007/0060097	A1 *	3/2007	Edge	 H04W 4/90	2011/0206039	A1 8/2011 Lee
					455/404.1	2011/0208801	A1 8/2011 Thorkelsson
	2007/0067828	A1	3/2007	Bychkov		2011/0231354	A1 9/2011 O'Sullivan
	2007/0074276	A1	3/2007	Harrison		2011/0265149	A1 10/2011 Ganesan
	2007/0077916	A1	4/2007	Saito		2011/0273551	A1 11/2011 Yang
	2007/0079135	A1	4/2007	Saito		2011/0287782	A1 11/2011 Ho et al.
						2012/0054831	A1 1/2012 Patvarczki
						2012/0124651	A1 5/2012 Ganesan
						2012/0166598	A1 6/2012 Yuan
						2012/0184291	A1 7/2012 Tietsch et al.

US 12,058,528 B2

Page 3

(56)

References Cited

U.S. PATENT DOCUMENTS

2012/0192255	A1	7/2012	Ganesan	
2012/0202517	A1	8/2012	Edge	
2012/0272056	A1	10/2012	Ganesan	
2013/0060665	A1 *	3/2013	Davis	H04L 9/40 707/E17.014
2013/0133086	A1	5/2013	Liberman	
2013/0165040	A1	6/2013	Mcintyre	
2013/0196685	A1	8/2013	Griff	
2013/0232547	A1	9/2013	Ganesan	
2013/0282589	A1	10/2013	Shoup	
2013/0333006	A1	12/2013	Tapling	
2014/0020073	A1	1/2014	Ronda	
2014/0189861	A1 *	7/2014	Gupta	H04L 63/08 709/224
2014/0199962	A1	7/2014	Mohammed	
2014/0273965	A1	9/2014	Raleigh	
2014/0282870	A1 *	9/2014	Markwordt	G06F 21/31 726/3
2014/0295886	A1	10/2014	Tickoo	
2014/0298432	A1	10/2014	Brown	
2014/0317689	A1	10/2014	Mogush	
2014/0359722	A1	12/2014	Schultz et al.	
2015/0043724	A1	2/2015	Farris	
2015/0106955	A1	4/2015	Soelberg et al.	
2015/0139407	A1 *	5/2015	Maguire	H04M 3/30 379/22.03
2015/0156267	A1	6/2015	Zhang	
2015/0254672	A1	9/2015	Huesch	
2015/0302397	A1	10/2015	Kalgi	
2016/0014603	A1	1/2016	Woodward	
2016/0036777	A1	2/2016	Bartlett	
2016/0112569	A1	4/2016	Timem	
2016/0125534	A1	5/2016	Baker	
2016/0127370	A1	5/2016	Hettervik	
2016/0148597	A1	5/2016	Hamid	
2016/0156620	A1	6/2016	Ganesan	
2016/0173687	A1	6/2016	Ehrlich	
2016/0191494	A1	6/2016	Claes	
2016/0255477	A1	9/2016	Parulski	
2016/0316341	A1	10/2016	Vaccari	
2016/0350751	A1	12/2016	Keys	
2017/0078859	A1	3/2017	Kendrick	
2017/0085568	A1 *	3/2017	Rolfe	H04L 63/06
2017/0085635	A1	3/2017	Nicholls	
2017/0123069	A1	5/2017	Kotab	
2017/0149769	A1	5/2017	Ganesan	
2017/0235454	A1	8/2017	Selfridge	
2017/0238129	A1 *	8/2017	Maier	H04W 4/029 455/404.2
2017/0289172	A1	10/2017	Turakhia	
2017/0311367	A1	10/2017	Ursitti	
2017/0351977	A1	12/2017	Bijor	
2017/0352250	A1	12/2017	De Barros Chapiewski	
2017/0364911	A1	12/2017	Landrok	
2018/0013559	A1	1/2018	Hassan	
2018/0212971	A1	7/2018	Costa	
2019/0007553	A1	1/2019	Noldus	
2019/0080155	A1 *	3/2019	Ganong	G06V 40/167
2019/0208354	A1	7/2019	Raduchel	
2019/0238531	A1	8/2019	Ganesan	
2020/0042685	A1	2/2020	Tussy et al.	
2020/0167453	A1	5/2020	Bouse	
2020/0210988	A1	7/2020	Woodward	
2020/0364366	A1 *	11/2020	Kundu	H04L 63/102
2020/0366671	A1 *	11/2020	Larson	H04L 9/3228
2020/0382364	A1 *	12/2020	Kilburn	H04M 7/0024
2021/0044161	A1	2/2021	Kantorowicz	
2021/0044616	A1 *	2/2021	Kantorowicz	H04W 12/48
2021/0058507	A1	2/2021	Cornwell	
2021/0105271	A1 *	4/2021	Nitturkar	H04W 12/06
2021/0168148	A1 *	6/2021	Boodaei	H04L 63/0861
2022/0012743	A1 *	1/2022	Snell	H04W 12/72

FOREIGN PATENT DOCUMENTS

JP	2001175599	A	6/2001
JP	2002259344	A	9/2002
JP	2003186838	A	7/2003
JP	2005209083	A	8/2005
JP	2006221440	A	8/2006
JP	2007102777	A	4/2007
JP	2007328381	A	12/2007
JP	2013518348	A	5/2013
WO	WO2007026486		3/2007
WO	WO2007103831		9/2007
WO	WO2007107868		9/2007
WO	WO2008123461		10/2008

OTHER PUBLICATIONS

U.S. Appl. No. 17/246,471: Non-Final Office Action dated Apr. 13, 2023, 48 pages, Doc 1890.

U.S. Appl. No. 18/076,074: Filing Receipt & Miscellaneous Communication to Applicant date Dec. 23, 2022, 4 pages, Doc 1891.

PCT Application No. PCT/US2022/052028: Intl Search Report and Written Opinion dated Apr. 13, 2023, 24 pages, Doc 1894.

U.S. Appl. No. 18/185,605: Patent Application filed Mar. 17, 2023, 59 pages, Doc 1892.

Anton—"Kodekey Biometric Authentication System Links Your Identity to Your Phone Number", TECHTHELEAD.com, Jan. 30, 2006, 6 pages, Doc 1212.

Burr—"Maximizing Consumer Contacts while Mitigating TCPA Risk", Mar. 12, 2014, available at: <https://www.neustar.biz/resources/videos/mitigate-tcpa-risk-aml-connections-video>, 18 pages, Doc 1215.

Dryburgh, et al.; "Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services"; Cisco Press, Aug. 2, 2004 available at: <http://itechbus.safaribooksonline.com/book/e?ectrica!-engineeringcommunication1H,engineering/1587050404/introductions-and-overviewsichi.13>, 2 pages, Doc 1217.

Federal Communications Commission; "Wireless Local Number Portability (WLNP)—frequently asked questions"; May 18, 2016; available at: <https://wireless.fcc.gov/wlnp/documents/wlnpfaqs.pdf>, pages, Doc 1214.

Gralla; "How the Internet Works"; 2006; Que, pp. 346-347, Doc 1233.

Gueye—"Constraint-Based Geolocation of Internet Hosts", IEEE/ACM Transactions on Networking, vol. 14, No. 6, Dec. 2006, 14 pages, Doc 1210.

IP2LOCATION—"Identify Geographical Location and Proxy by IP Address", (<http://www.ip2location.com>), 2001, 6 pages, Doc 1208.

Katz-Bassett—"Towards IP Geolocation Using Delay and Topology Measurements" IMC'06, Oct. 25-27, 2006, Rio de Janeiro, Brazil, 13 pages, Doc 1211.

Malphrus; "Perspectives on Retail Payments Fraud"; Feb. 11, 2009, Economic Perspectives, vol. XXXIII, No. 1, 2009; available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1341233, 6 pages, Doc 1218.

Padmanabhan—"An Investigation of Geographic Mapping Techniques for Internet Hosts", SIGCOMM'01, Aug. 27-31, 2001, San Diego, CA, 13 pages, Doc 1209.

Quova "How we do it" (<http://www.quova.com/what/how-we-do-it/>), 2011, 3 pages, Doc 1250.

wiki.gis.com—Geolocation Software (http://en.wikipedia.org/wiki/Geolocation_software), Last Updated May 23, 2011, 4 pages, Doc 1207.

WOT Online; "How to interpret the reputation in reputation icon?"; 2006. Retrieved from http://web.archive.org/web/20061127233933/http://www.mywot.com/en/woUhelp/wot_symbols_explained, 3 pages, Doc 1213.

YTD2525—"Enterprise HLR Lookup Portal and API," published May 30, 2014 at blog YTD2525, citing hlr-lookups.com as the source, available at: <https://ytd2525.wordpress.com/2014/05/30/enterprise-hlr-lookup-portal-and-api/>, 5 pages, Doc 1216.

U.S. Appl. No. 17/031,696: US Patent Application filed Sep. 24, 2020, 65 pages, Doc 1219.

US 12,058,528 B2

Page 4

(56)

References Cited

OTHER PUBLICATIONS

U.S. Appl. No. 17/031,696: Filing Receipt dated Oct. 14, 2020, 3 pages, Doc 1220.
 U.S. Appl. No. 17/031,696: Non-final Office Action dated Sep. 15, 2021, 18 pages, Doc 1221.
 U.S. Appl. No. 17/031,696: Response to Office Action filed Jan. 11, 2022, 16 pages, Doc 1222.
 U.S. Appl. No. 17/031,696: Final Office Action dated Mar. 16, 2022, 32 pages, Doc 1223.
 PCT Application No. PCT/US2020/052580: PCT Application filed Sep. 24, 2020, 58 pages, Doc 1224.
 PCT Application No. PCT/US2020/052580: Intl Search Report and Written Opinion dated Dec. 8, 2020, 16 pages, Doc 1225.
 PCT Application No. PCT/US2020/052580: Article 34 Amendment filed Mar. 5, 2021, 20 pages, Doc 1226.
 PCT Application No. PCT/US2020/052580: Intl Preliminary Report on Patentability mailed Jan. 19, 2022, 20 pages, Doc 1227.
 U.S. Appl. No. 15/470,522: Patent Application filed Mar. 27, 2017, 48 pages, Doc 1228A and 1228B.
 U.S. Appl. No. 15/470,522: Preliminary Amendment filed Mar. 30, 2017, 8 pages, Doc 1229.
 U.S. Appl. No. 15/470,522: Filing Receipt and Notice to File Corrected Application Papers dated Apr. 4, 2017, 5 pages, Doc 1230.
 U.S. Appl. No. 15/470,522: Amendment and Response to Notice to File Corrected Application Papers filed Apr. 18, 2017, 53 pages, Doc 1231A and 1231B.
 U.S. Appl. No. 15/470,522: Updated Filing Receipt dated Apr. 18, 2017, 3 pages, Doc 1232.
 U.S. Appl. No. 15/470,522: Restriction Requirement dated Feb. 4, 2019, 8 pages, Doc 1234.
 U.S. Appl. No. 15/470,522: Amendment and Response to Restriction Requirement filed Apr. 1, 2019, 12 pages, Doc 1235.
 U.S. Appl. No. 15/470,522: Non-final Office Action dated May 16, 2019, 26 pages, Doc 1236.
 U.S. Appl. No. 15/470,522: Amendment filed Aug. 1, 2019, 12 pages, Doc 1237.
 U.S. Appl. No. 15/470,522: Notice of Allowance dated Dec. 30, 2019, 8 pages, Doc 1238.
 U.S. Appl. No. 15/470,522: Issue Fee Payment filed Dec. 30, 2019, 5 pages, Doc 1239.
 U.S. Appl. No. 15/470,522: Issue Notification dated Jan. 15, 2020, 1 page, Doc 1240.
 U.S. Appl. No. 16/730,878: Patent Application filed Dec. 30, 2019, 49 pages, Doc 1241A and 1241B.
 U.S. Appl. No. 16/730,878: Filing Receipt and Notice to File Corrected Application Papers dated Jan. 24, 2020, 6 pages, Doc 1242.
 U.S. Appl. No. 16/730,878: Amendment and Response to Notice to File Corrected Application Papers filed Mar. 24, 2020, 39 pages, Doc 1243A and 1243B.
 U.S. Appl. No. 16/730,878: Updated Filing Receipt dated Mar. 26, 2020, 4 pages, Doc 1244.
 U.S. Appl. No. 16/730,878: Notice of Publication dated Jul. 6, 2020, 1 page, Doc 1245.
 U.S. Appl. No. 16/730,878: Request for Corrected Filing Receipt dated Jul. 9, 2020, 1 page, Doc 1246.
 U.S. Appl. No. 16/730,878: Corrected Filing Receipt dated Jul. 13, 2020, 4 pages, Doc 1247.
 U.S. Appl. No. 12/938,245: Patent Application filed Nov. 2, 2010, 24 pages, Doc 1248.
 U.S. Appl. No. 12/938,245: Filing Receipt dated Nov. 17, 2020, 3 pages, Doc 1249.
 U.S. Appl. No. 12/938,245: Preliminary Amendment filed Jan. 10, 2012, 17 pages, Doc 1251.
 U.S. Appl. No. 12/938,245: Examiner Initiated Interview Summary and Notice of Allowance dated Jun. 18, 2012, 22 pages, Doc 1252.
 U.S. Appl. No. 12/938,245: Issue Fee Payment filed Nov. 8, 2012, 1 page, Doc 1253.

U.S. Appl. No. 12/938,245: Issue Notification dated Dec. 5, 2012, 1 page, Doc 1254.
 U.S. Appl. No. 13/669,123: Patent Application filed Nov. 5, 2012, 83 pages, Doc 1255A-D.
 U.S. Appl. No. 13/669,123: Filing Receipt and Notice to File Corrected Application Papers dated Dec. 4, 2012, 5 pages, Doc 1256.
 U.S. Appl. No. 13/669,123: Amendment and Response to Notice to File Corrected Application Papers filed Jan. 8, 2013, 4 pages, Doc 1257.
 U.S. Appl. No. 13/669,123: Updated Filing Receipt dated Aug. 12, 2013, 3 pages, Doc 1258.
 U.S. Appl. No. 13/669,123: Notice of Allowance dated Sep. 11, 2013, 10 pages, Doc 1259.
 U.S. Appl. No. 13/669,123: Issue Fee Payment filed Oct. 14, 2013, 2 pages, Doc 1260.
 U.S. Appl. No. 13/669,123: Issue Notification dated Oct. 30, 2013, 1 page, Doc 1261.
 U.S. Appl. No. 13/736,944: Patent Application filed Jan. 9, 2013, 17 pages, Doc 1262.
 U.S. Appl. No. 13/736,944: Filing Receipt dated Feb. 6, 2014, 3 pages, Doc 1263.
 U.S. Appl. No. 13/736,944: Non-final Office Action dated May 4, 2013, 16 pages, Doc 1264.
 U.S. Appl. No. 13/736,944: Response to Non-final Office Action filed Dec. 9, 2015, 12 pages, Doc 1265.
 U.S. Appl. No. 13/736,944: Final Office Action dated Oct. 6, 2016, 18 pages, Doc 1266.
 U.S. Appl. No. 13/736,944: Request for Continued Examination and Amendment filed Apr. 4, 2017, 14 pages, Doc 1267.
 U.S. Appl. No. 13/736,944: Advisory Action dated Apr. 28, 2017, 4 pages, Doc 1268.
 U.S. Appl. No. 13/736,944: Request for Continued Examination filed May 1, 2017, 6 pages, Doc 1269.
 U.S. Appl. No. 13/736,944: Corrected Filing Receipt dated May 4, 2017, 3 pages, Doc 1270.
 U.S. Appl. No. 13/736,944: Replacement Filing Receipt dated May 26, 2017, 3 pages, Doc 1271.
 U.S. Appl. No. 13/736,944: Non-final Office Action dated Mar. 21, 2018, 47 pages, Doc 1272A and 1272B.
 U.S. Appl. No. 13/736,944: Amendment and Terminal Disclaimer filed Jun. 21, 2018, 42 pages, Doc 1273.
 U.S. Appl. No. 13/736,944: Final Office Action dated Oct. 18, 2018, 37 pages, Doc 1274.
 U.S. Appl. No. 13/736,944: Response to Final Office Action filed Dec. 17, 2018, 15 pages, Doc 1275.
 U.S. Appl. No. 13/736,944: Advisory Action dated Jan. 14, 2019, 6 pages, Doc 1276.
 U.S. Appl. No. 13/736,944: Notice of Appeal, pages, Doc 1277.
 U.S. Appl. No. 13/736,944: Appeal Brief filed Mar. 18, 2019, 20 pages, Doc 1278.
 U.S. Appl. No. 13/736,944: Notice of Allowance dated Jul. 8, 2019, 19 pages, Doc 1279.
 U.S. Appl. No. 13/736,944: Issue Fee Payment filed Oct. 3, 2019, 4 pages, Doc 1280.
 U.S. Appl. No. 13/736,944: Issue Notification dated Feb. 19, 2020, 1 page, Doc 1281.
 U.S. Appl. No. 15/422,137: Patent Application filed Feb. 1, 2017, 46 pages, Doc 1282A and 1282B.
 U.S. Appl. No. 15/422,137: Filing Receipt and Notice to File Missing Parts dated Feb. 13, 2017, 7 pages, Doc 1283.
 U.S. Appl. No. 15/422,137: Response to Notice to File Missing Parts filed Apr. 11, 2017, 6 pages, Doc 1284.
 U.S. Appl. No. 15/422,137: Updated Filing Receipt dated Apr. 14, 2017, 4 pages, Doc 1285.
 U.S. Appl. No. 15/422,137: Notice of Publication dated May 25, 2017, 1 page, Doc 1312.
 U.S. Appl. No. 15/422,137: Non-final Office Action dated Sep. 20, 2018, 28 pages, Doc 1286.
 U.S. Appl. No. 15/422,137: Response to Non-final Office Action filed Dec. 19, 2018, 17 pages, Doc 1313.
 U.S. Appl. No. 15/422,137: Applicant Initialed Interview Summary dated Dec. 21, 2018. 4 pages, Doc 1314.

US 12,058,528 B2

Page 5

(56)

References Cited

OTHER PUBLICATIONS

U.S. Appl. No. 15/422,137: Non-final Office Action dated Apr. 11, 2019, 28 pages, Doc 1315.
 U.S. Appl. No. 5/422,137: Response to Non-final Office Action filed Jul. 9, 2019, 15 pages, Doc 1316.
 U.S. Appl. No. 15/422,137: Notice of Allowance dated Oct. 25, 2019, 20 pages, Doc 1317.
 U.S. Appl. No. 15/422,137: Issue Fee Payment filed Jan. 21, 2020, 3 pages, Doc 1318.
 U.S. Appl. No. 15/422,137: Issue Notification dated Feb. 12, 2020, 1 page, Doc 1319.
 U.S. Appl. No. 16/790,394: Patent Application filed Feb. 13, 2020, 43 pages, Doc 1300.
 U.S. Appl. No. 16/790,394: Filing Receipt and Notice of Missing Parts dated Mar. 3, 2020, 6 pages, Doc 1301.
 U.S. Appl. No. 16/790,394: Preliminary Amendment and Response to Notice of Missing Parts filed May 29, 2020, 13 pages, Doc 1302.
 U.S. Appl. No. 16/790,394: Updated Filing Receipt dated Jun. 4, 2020, 4 pages, Doc 1303.
 U.S. Appl. No. 16/790,394: Request for Corrected Filing Receipt filed Jul. 17, 2020, 1 pages, Doc 1304.
 U.S. Appl. No. 16/790,394: Corrected Filing Receipt dated Jul. 21, 2020, 4 pages, Doc 1305.
 U.S. Appl. No. 16/790,394: Notice of Publication dated Sep. 10, 2020, 1 page, Doc 1306.
 U.S. Appl. No. 16/790,394: Non-final Office Action dated May 17, 2021, 26 pages, Doc 1307.
 U.S. Appl. No. 16/790,394: Amendment and Terminal Disclaimer filed Aug. 10, 2021, 22 pages, Doc 1308.
 U.S. Appl. No. 16/790,394: Office Action dated Nov. 18, 2021, 31 pages, Doc 1309.
 U.S. Appl. No. 16/790,394: Response to Office Action filed Feb. 18, 2022, 16 pages, Doc 1310.
 U.S. Appl. No. 16/790,394: Final Office Action dated Apr. 13, 2022, 33 pages, Doc 1311.
 U.S. Appl. No. 17/558,570: Patent Application filed Dec. 21, 2021, 80 pages, Doc 1287.
 U.S. Appl. No. 17/558,570: Filing Receipt dated Jan. 5, 2022, 4 pages, Doc 1288.
 U.S. Appl. No. 17/558,570: Notice of Missing Parts dated Jan. 5, 2022, 2 pages, Doc 1289.
 U.S. Appl. No. 17/558,570: Response to Notice of Missing Parts filed Mar. 7, 2022, 6 pages, Doc 1290.
 PCT Application PCT/US2021/065112: PCT Application filed Dec. 23, 2021, 67 pages, Doc 1291.
 PCT Application PCT/US21/65799: PCT Application filed Dec. 30, 2021, 80 pages, Doc 1296.
 U.S. Appl. No. 17/246,471: Patent Application filed Apr. 30, 2021, 73 pages, Doc 1297.
 U.S. Appl. No. 17/246,471: Filing Receipt dated May 11, 2021, 4 pages, Doc 1298.
 PCT Application PCT/US22/26637: PCT Application filed Apr. 28, 2022, 63 pages, Doc 1299.
 U.S. Appl. No. 17/031,696: Notice of Abandonment dated May 26, 2023, 2 pages, Doc 1937.
 U.S. Appl. No. 16/730,878: AFCP Request & Response to Final dated May 30, 2023, 20 pages, Doc 1938.
 U.S. Appl. No. 16/730,878: Advisory Action dated Jun. 13, 2023, 5 pages, Doc 1939.
 U.S. Appl. No. 16/730,878: RCE & Amendment filed Jun. 28, 2023, 23 pages, Doc 1940.

BR Application No. 1120230126002: Brazil Application filed Jun. 22, 2023, 107 pages, Doc 1941.
 CA Application No. 3202486: Canada Application filed Jun. 15, 2023, 2 pages, Doc 1942.
 EP Application No. 21912241.3: European Application filed Jun. 15, 2023, 6 pages, Doc 1943.
 EP Application No. 21912241.3: Rule 161-162 Communication dated Aug. 1, 2023, 3 pages, Doc 1944.
 IN Application No. 202347042104: India Application filed Jun. 23, 2023, 65 pages, Doc 1945.
 BR Application No. 1120230131685: Brazil Application filed Jun. 29, 2023, 120 pages, Doc 1946.
 CA Application No. 3202488: Canada Application filed Jun. 15, 2023, 2 pages, Doc 1947.
 EP Application No. 21916545.3: European Application filed Jun. 15, 2023, 6 pages, Doc 1948.
 EP Application No. 21916545.3: Rule 161-162 Communication dated Aug. 8, 2023, 3 pages, Doc 1949.
 IN Application No. 202347042972: India Application filed Jun. 27, 2023, 78 pages, Doc 1950.
 U.S. Appl. No. 18/076,074: Notice of Publication dated Jun. 8, 2023, 1 page, Doc 1951.
 PCT Application No. PCT/US2021/065799: International Search Report and Written Opinion dated May 5, 2022, 24 pages, Doc 1830.
 PCT Application No. PCT/US2022/26637: International Search Report and Written Opinion dated Jul. 18, 2022, 24 pages, Doc 1829.
 U.S. Appl. No. 17/558,570: Notice of Publication dated Jun. 23, 2022, 1 page, Doc 1832.
 U.S. Appl. No. 17/565,427: Notice of Publication dated Jun. 30, 2022, 1 page, Doc 1831.
 U.S. Appl. No. 17/031,696: Response to Final Office Action filed May 6, 2022, 18 pages, Doc 1349.
 U.S. Appl. No. 17/031,696: Advisory Action dated May 13, 2022, 3 pages, Doc 1350.
 U.S. Appl. No. 17/031,696: Rce & Response to Final Office Action filed Jun. 6, 2022, 20 pages, Doc 1865.
 U.S. Appl. No. 17/031,696: Non-final Office Action dated Jun. 20, 2022, 21 pages, Doc 1866.
 U.S. Appl. No. 17/031,696: Response to Non-Final Office Action filed Sep. 9, 2022, 15 pages, Doc 1867.
 U.S. Appl. No. 17/031,696: Non-final Office Action dated Nov. 18, 2022, 39 pages, Doc 1863.
 U.S. Appl. No. 16/730,878: Non-final Office Action dated Sep. 22, 2022, 38 pages, Doc 1848.
 PCT Application No. PCT/US2021/065112: International Search Report and Written Opinion dated Mar. 22, 2022, 24 pages, Doc 1847.
 U.S. Appl. No. 17/246,471: Notice of Publication date Nov. 3, 2022, 1 page, Doc 1864.
 PCT Application No. PCT/US2021/065112: Response to Written Opinion filed Oct. 21, 2022, 7 pages, Doc 1877.
 PCT Application No. PCT/US2021/065799: Demand & Response to Written Opinion filed Oct. 28, 2022, 30 pages, Doc 1878.
 U.S. Appl. No. 16/730,878: Response to Non-Final Office Action filed Dec. 19, 2022, 17 pages, Doc 1872.
 U.S. Appl. No. 18/076,074, filed Dec. 6, 2022, 64 pages, Doc 1879.
 PCT Application No. PCT/US2022/052028: PCT Application filed Dec. 6, 2022, 63 pages, Doc 1868.

* cited by examiner

U.S. Patent

Aug. 6, 2024

Sheet 1 of 10

US 12,058,528 B2

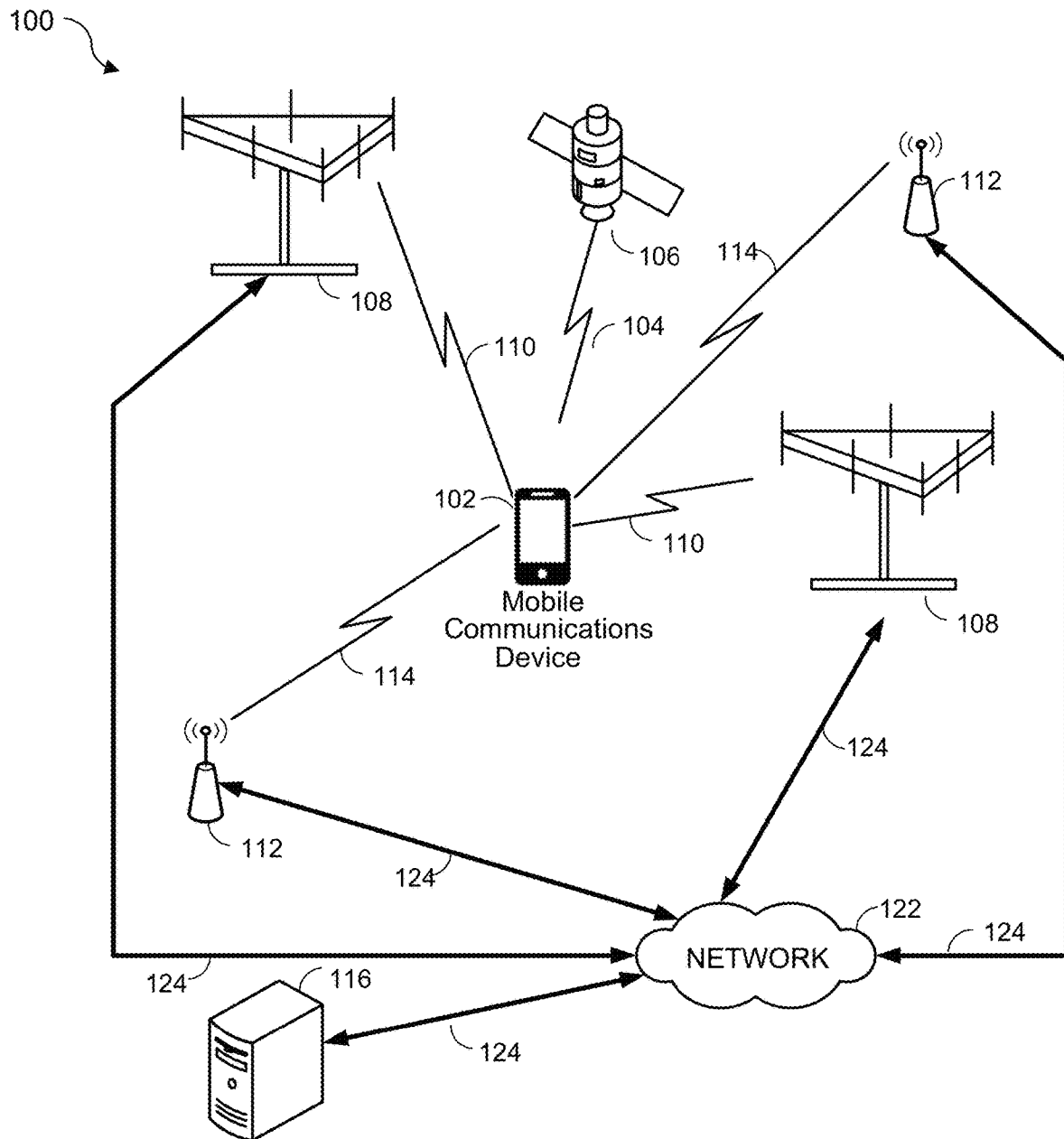
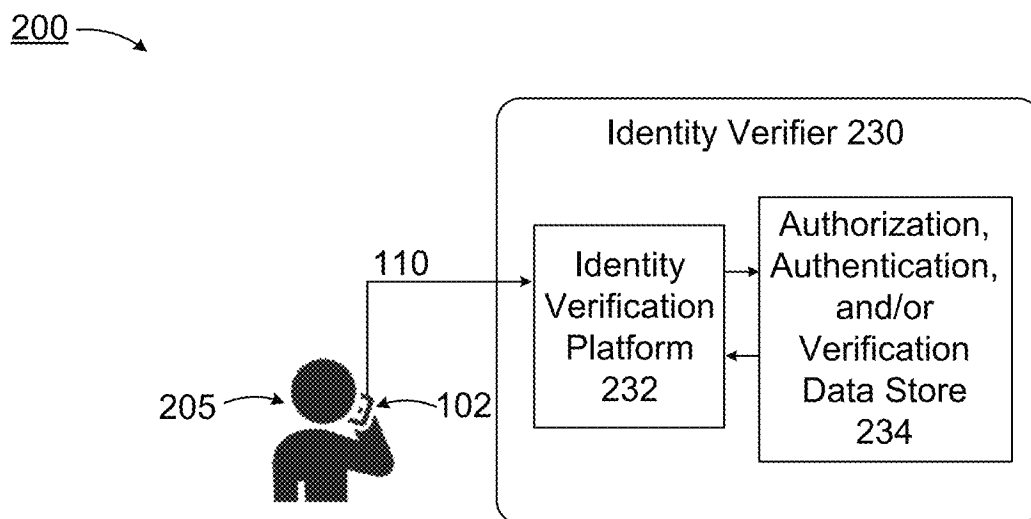
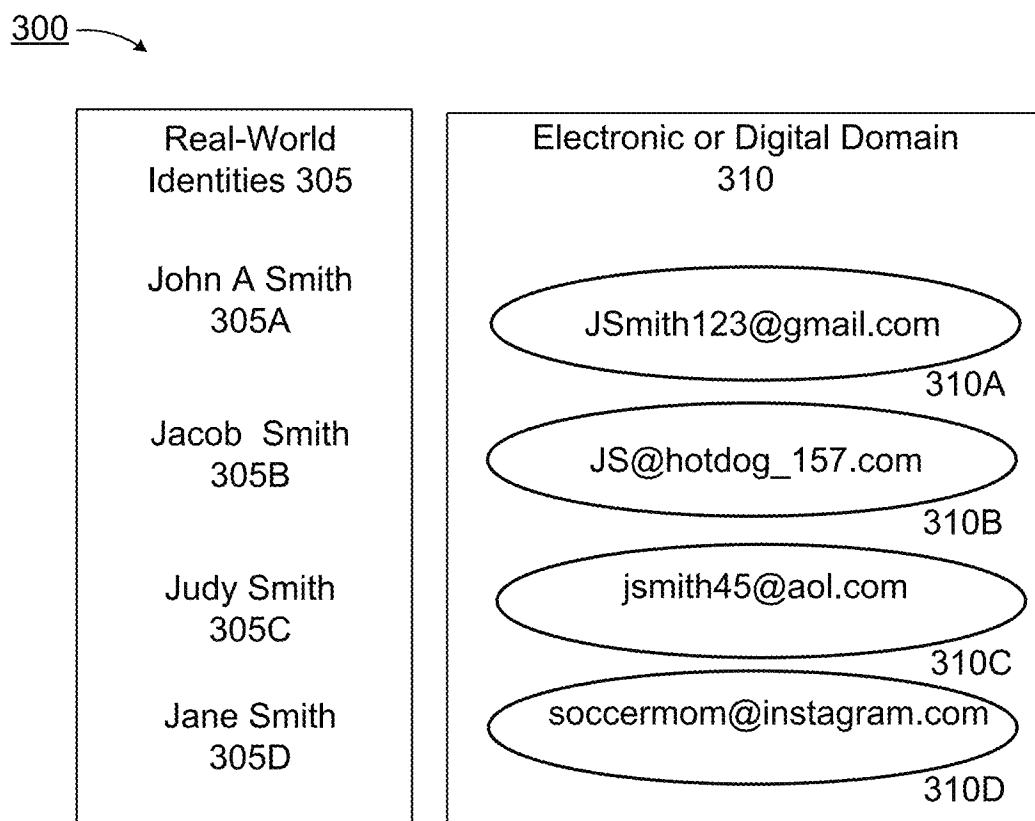


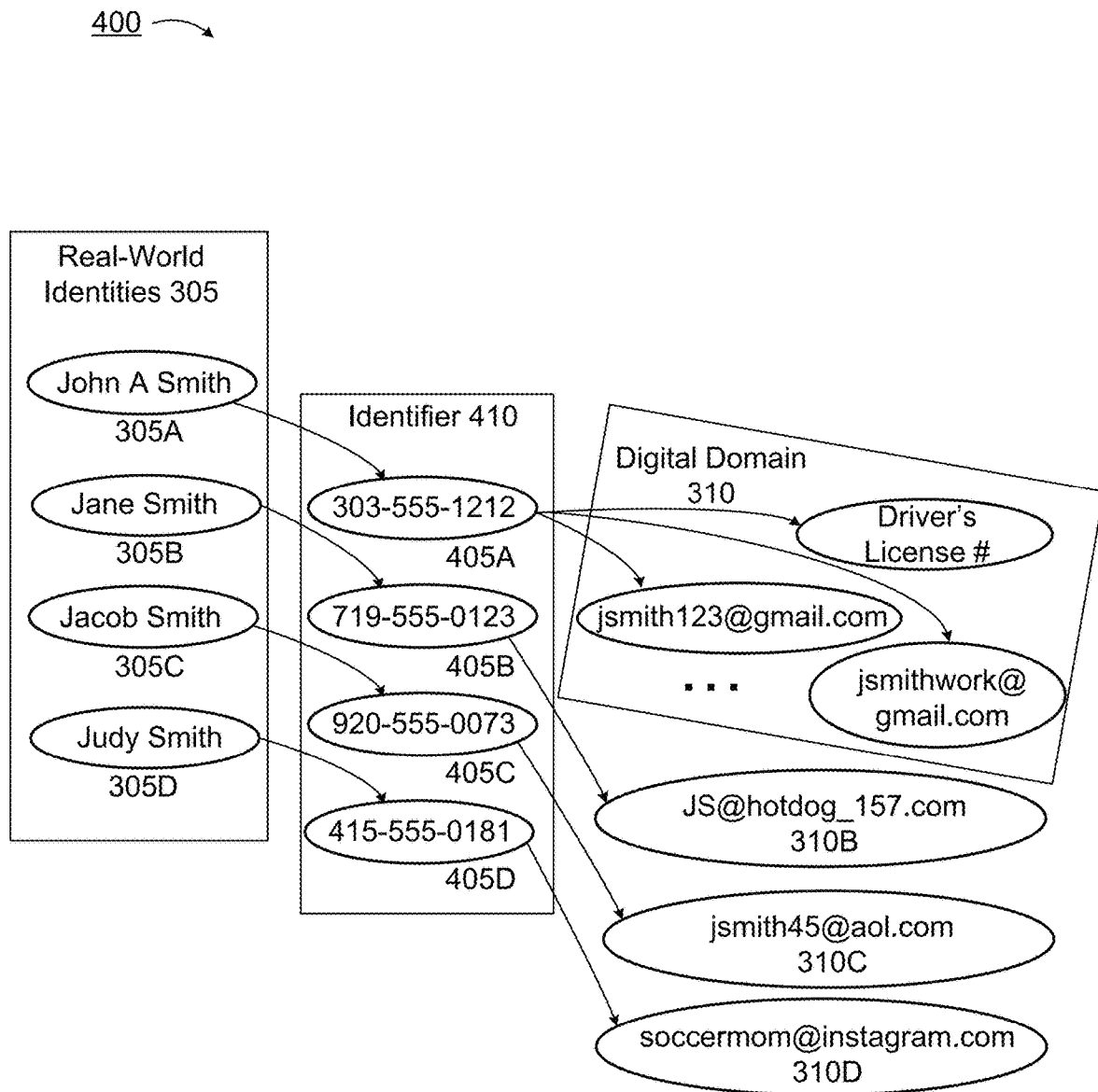
FIG. 1

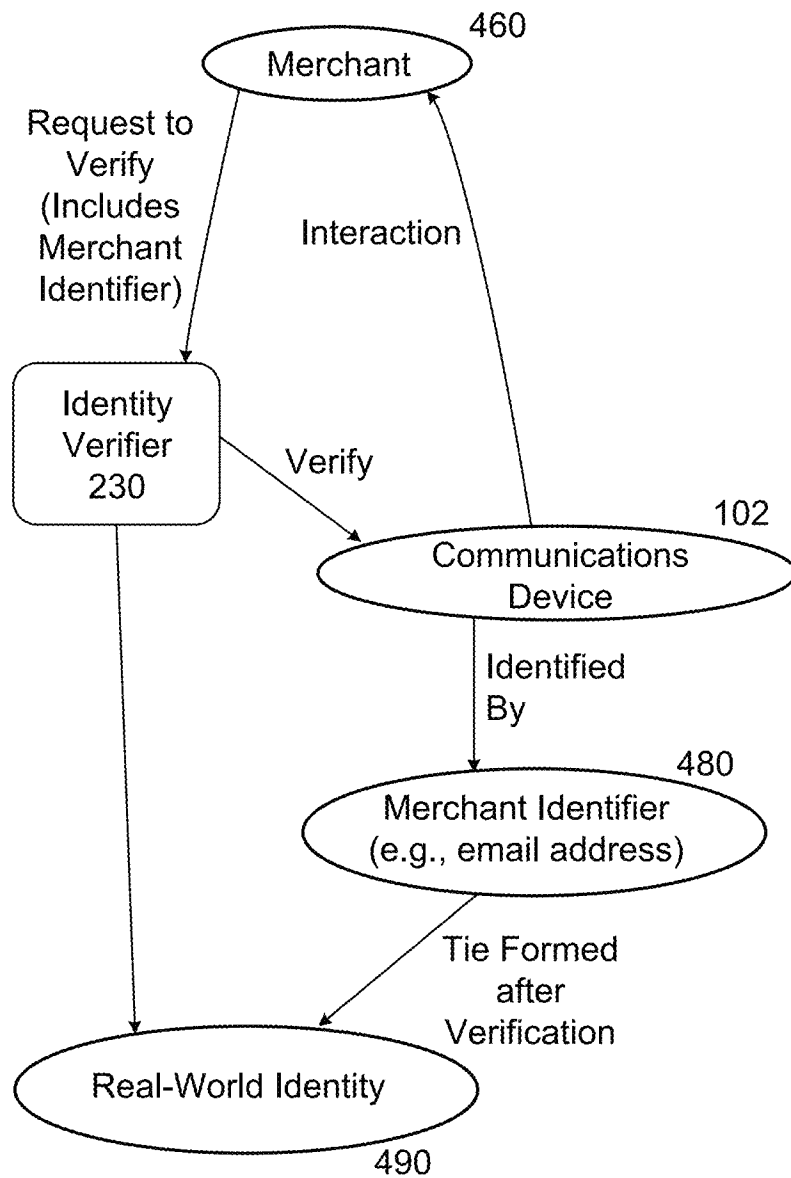
U.S. Patent

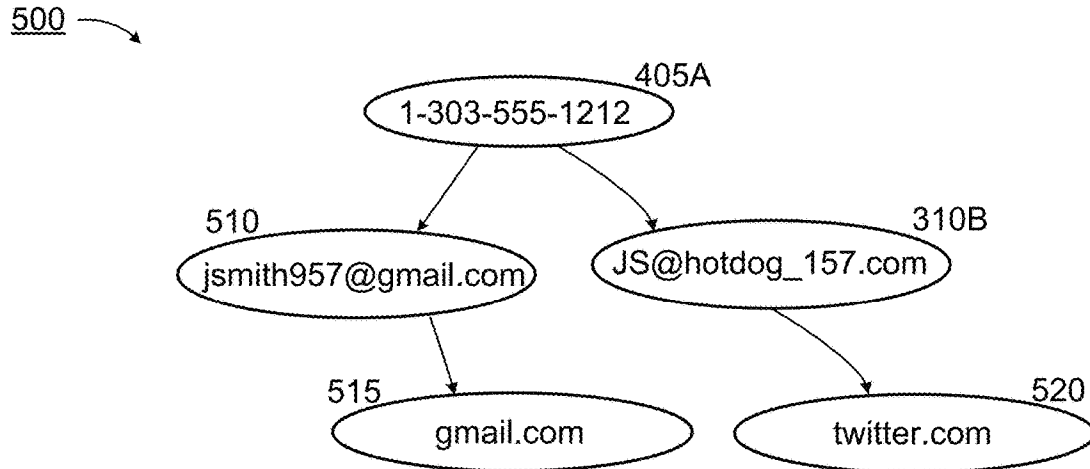
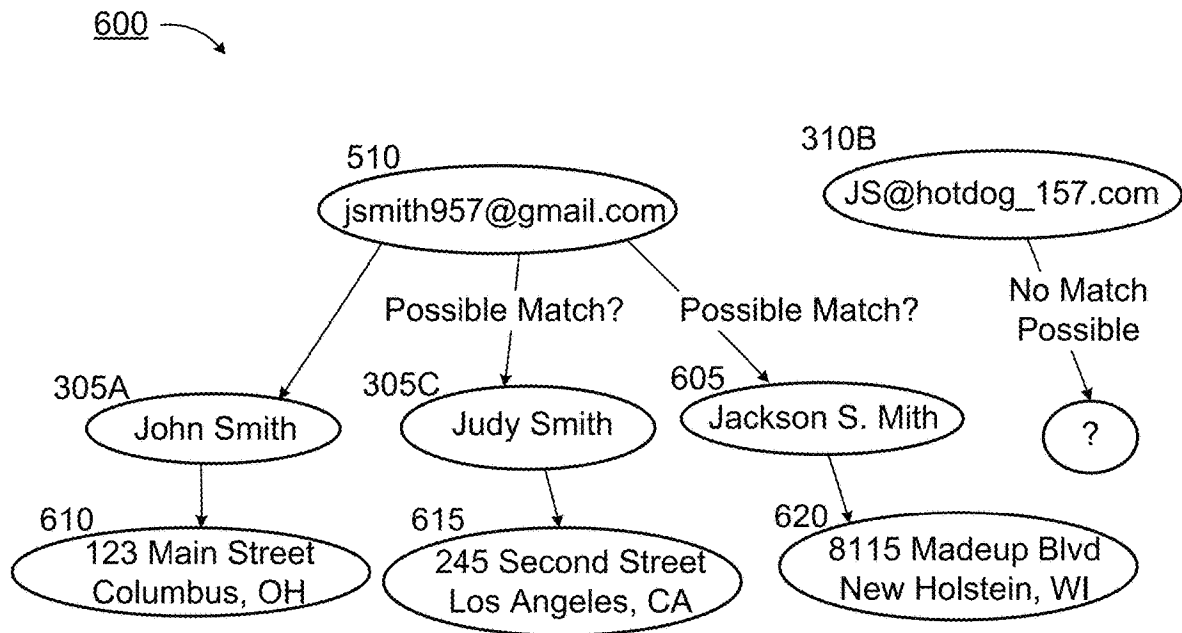
Aug. 6, 2024

Sheet 2 of 10

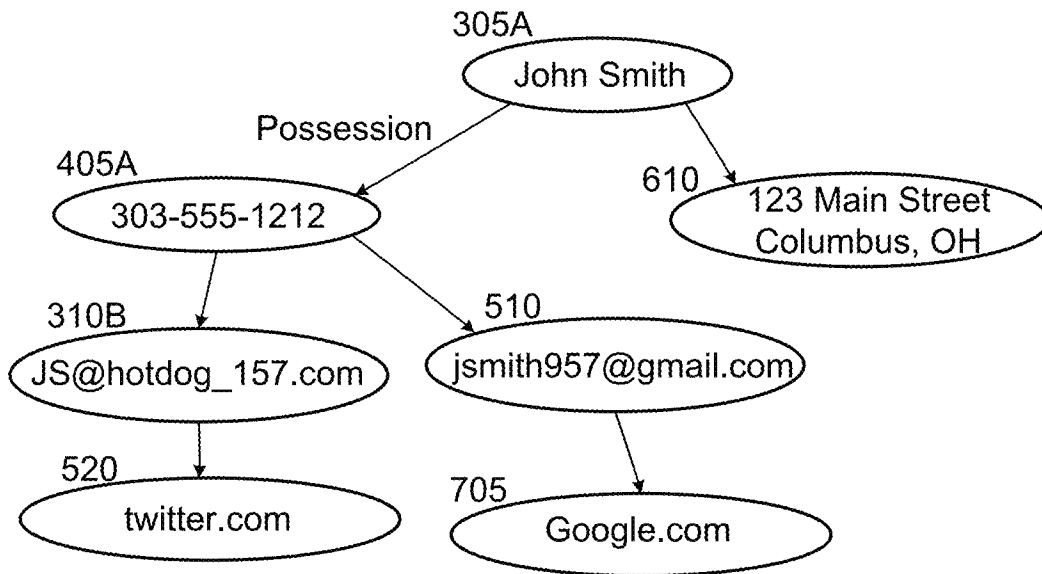
US 12,058,528 B2**FIG. 2****FIG. 3**

**FIG. 4A**

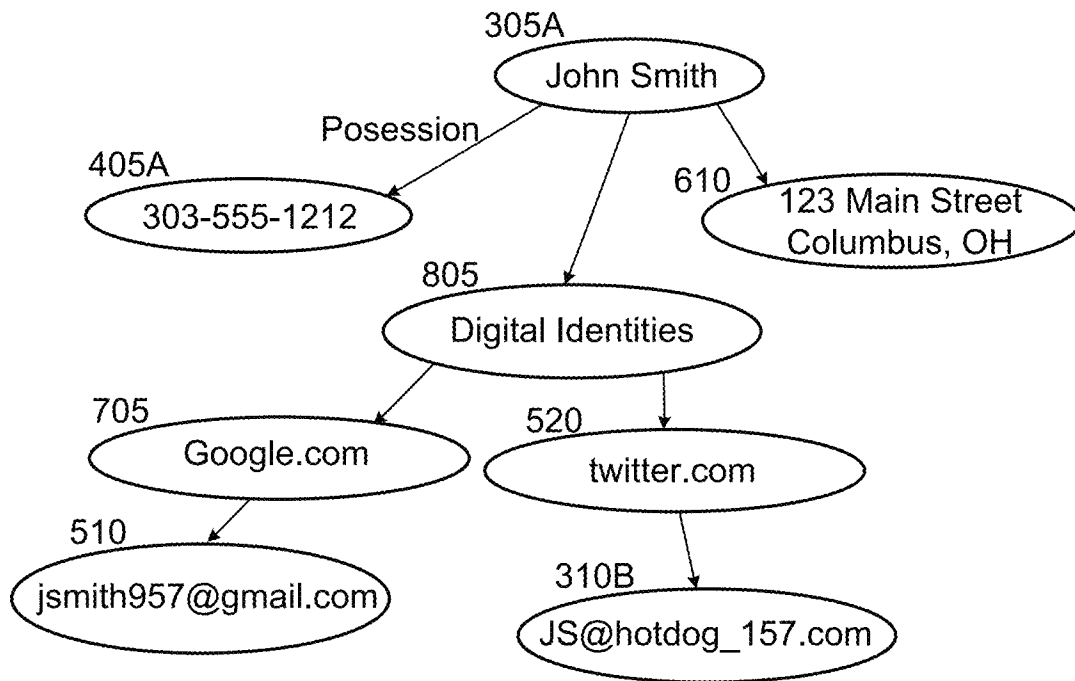
450 →**FIG. 4B**

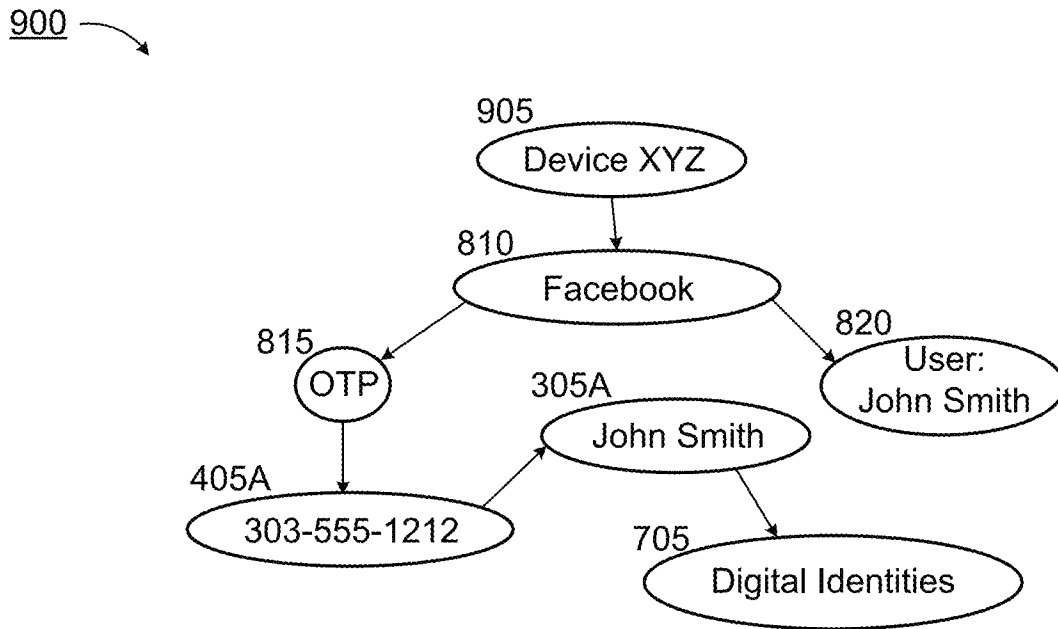
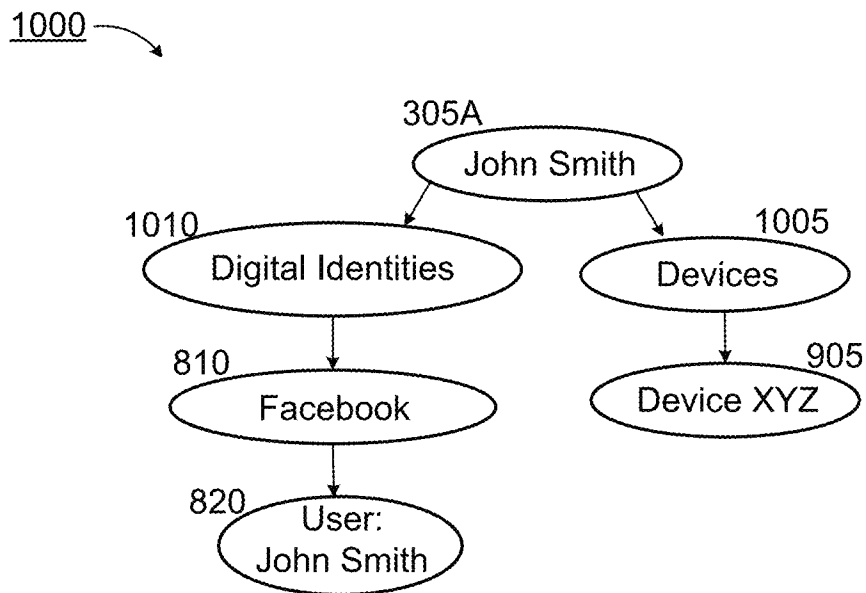
**FIG. 5****FIG. 6**

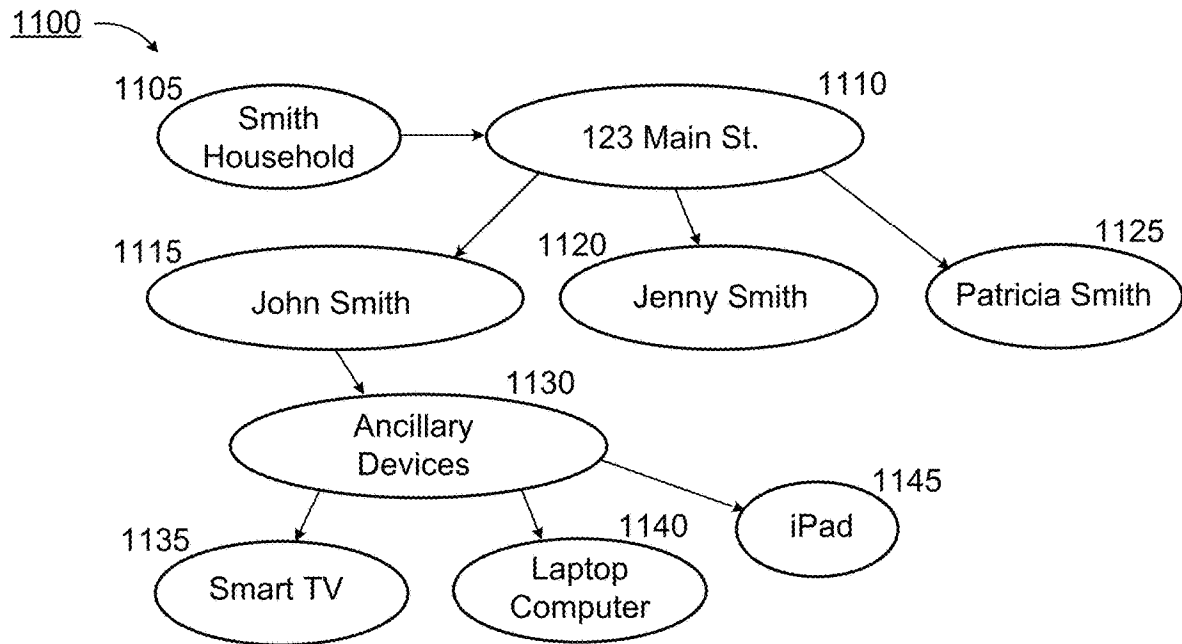
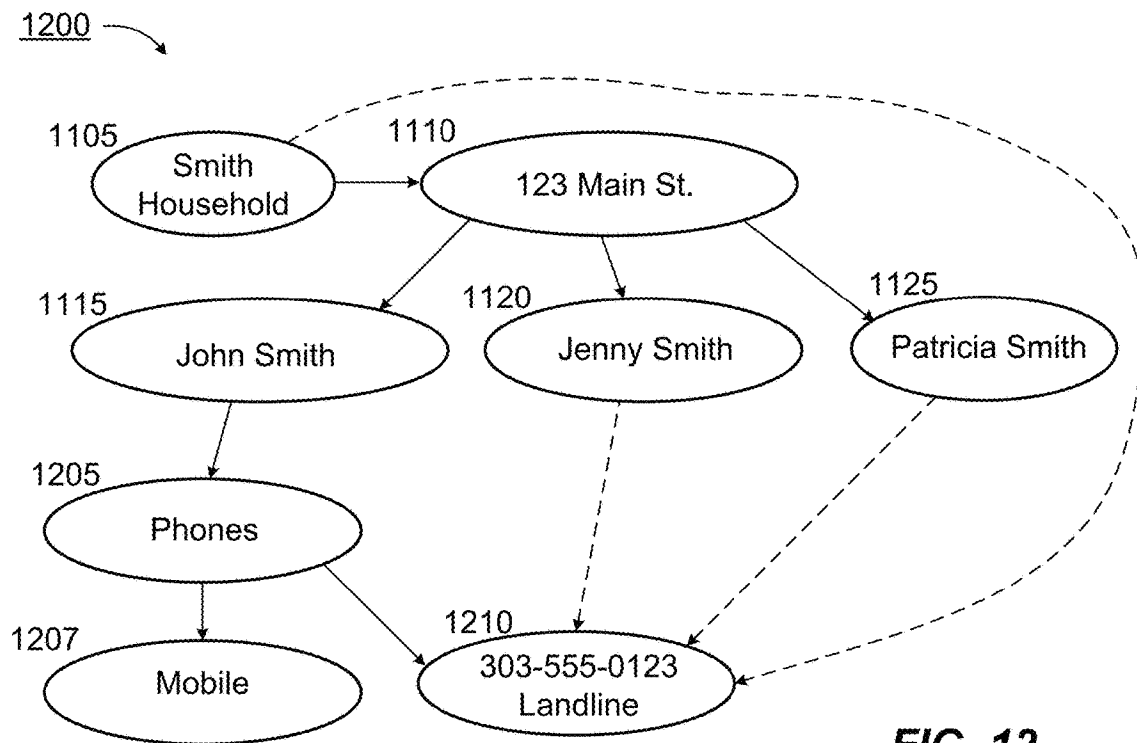
700

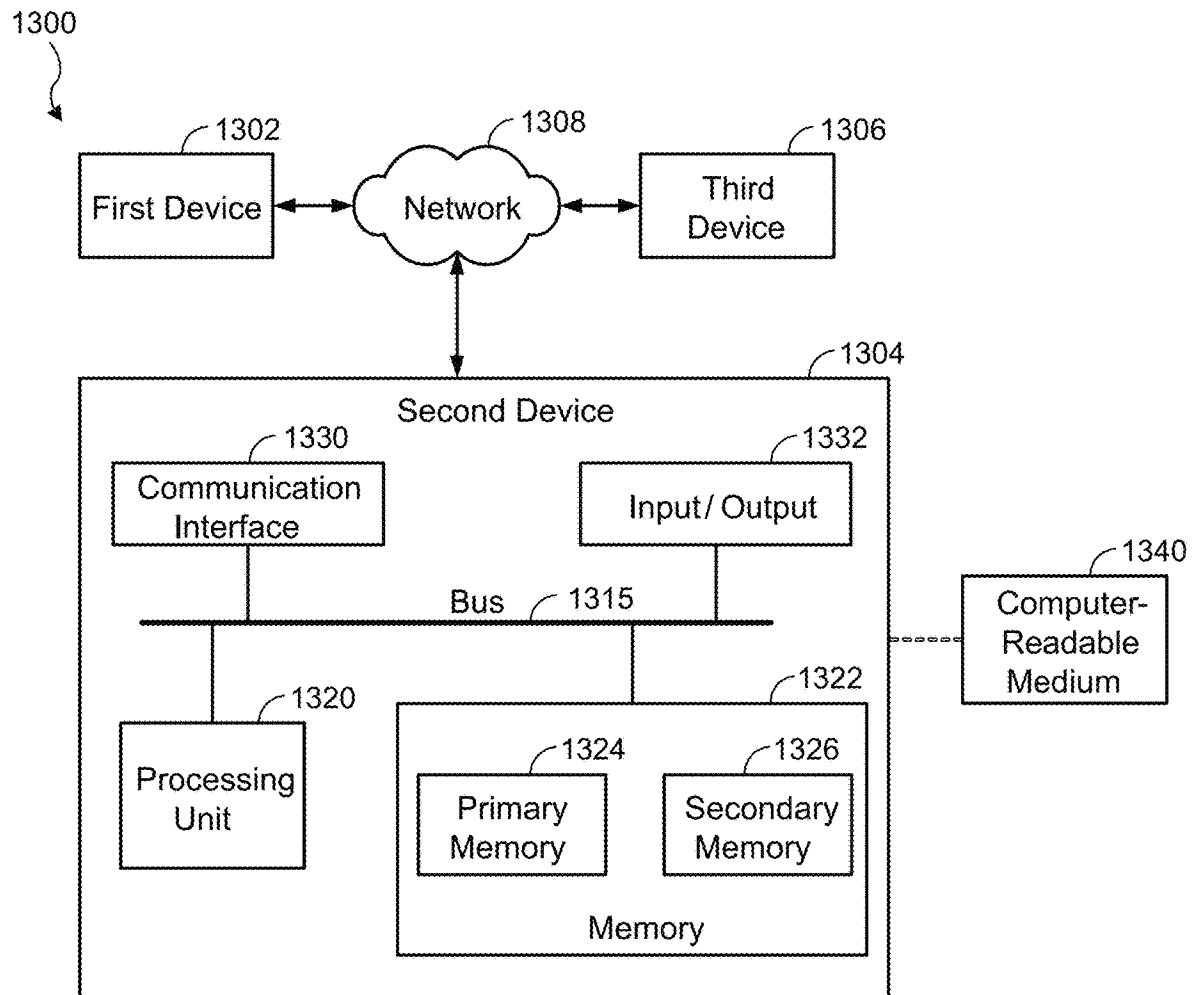
**FIG. 7**

800

**FIG. 8**

**FIG. 9****FIG. 10**

**FIG. 11****FIG. 12**

**FIG. 13**

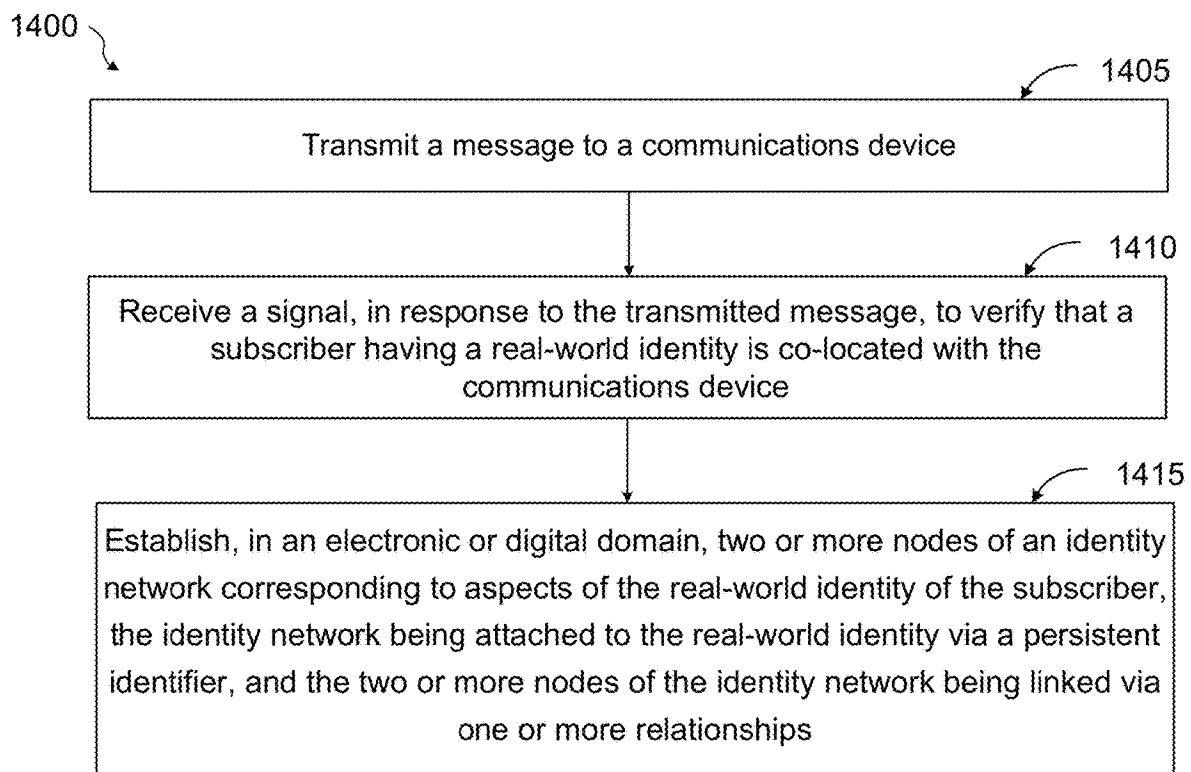


FIG. 14

US 12,058,528 B2

1

IDENTITY NETWORK REPRESENTATION OF COMMUNICATIONS DEVICE SUBSCRIBER IN A DIGITAL DOMAIN

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. provisional patent application Ser. No. 63/133,127, filed Dec. 31, 2020, which is incorporated by reference in its entirety and for all purposes.

BACKGROUND

1. Field

The present disclosure relates generally to electronic and/or communication infrastructures and, more particularly, to the formation and electronic storage, in an electronic or digital domain, of a subscriber's real-world identity via an identity network.

2. Information

The World Wide Web or simply the Web, as enabled by Internet computing, routing, and/or wireless transmission resources, has grown rapidly in recent years at least partially in response to the relative ease with which a wide variety of transactions can be performed or enabled via the Internet. As a consequence of widely available Internet connections, including connections to the Internet facilitated by wireless mobile communication services, for example, a mobile subscriber may shop and/or purchase virtually any product or service utilizing a handheld communications device. However, in such an environment, in which electronic, Internet-based commerce has become increasingly common, occurrences of fraud and deception, unfortunately, can also occur.

In addition to facilitating communications among devices having a primary purpose that relates to providing communication services, such as mobile cellular communications devices, the Web also facilitates communication among devices providing other functionalities, such as appliances, industrial, commercial, and household machines, control devices, sensors, etc. In such environments, which include an "Internet of things" (IOT) environment, as well as environments involving devices designed primarily for communications, instances of fraud and deception may bring theft of financial assets, intrusion by unauthorized parties into a user's home network, theft of privileged content, financial and/or credit fraud, and so forth. To reduce a likelihood of fraud, theft, or intrusion by unauthorized parties, fraud-detection and/or user authentication processes may be implemented. Thus, it may be appreciated that reduction in the instances of fraud and deception, which may involve, for example, use of various types of communications devices, continues to be an active area of investigation.

SUMMARY

A general embodiment may be directed to, a method may include transmitting a message to a communications device. The method also may also include receiving a signal, in response to the transmitted message, to verify that a subscriber having a real-world identity is co-located with the communications device. The method also may also include establishing, in an electronic or digital domain, two or more

2

nodes of an identity network corresponding to aspects of the real-world identity of the subscriber, the identity network being attached to the real-world identity via a persistent identifier, and the two or more nodes of the identity network being linked via one or more relationships.

In a particular embodiment, the method may further include establishing one or more additional nodes of the identity network responsive to electronically determining an aspect of the electronic or digital domain corresponding to the subscriber, the aspect including one or more of an electronic mail address of the real-world identity, an internet protocol address of the real-world identity, a wireline telephone number of the real-world identity, an identifier of an ancillary device, an institutional account in the name of the real-world identity, a healthcare account, or a transaction account of the real-world identity. In a particular embodiment, the method may further include establishing one or more additional relationships between or among the one or more nodes of the identity network responsive to one or more electronically determined events that occur with respect to the real-world identity. In a particular embodiment, the one or more electronically determined events correspond to one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, the healthcare account, and/or the transaction account in the name of the real-world identity. In a particular embodiment, the method may further include assigning a confidence score to the real-world identity in the electronic or digital domain. In a particular embodiment, the method may further include revising the confidence score based, at least in part, on the one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, and/or the transaction account in the name of the real-world identity. In a particular embodiment, the confidence score is based, at least in part, on one or more deterministic events with respect to the communications device. In a particular embodiment, the method may further include accessing a data store to detect one or more deterministic events in relation to historical norms with respect to the communications device corresponding to the real-world identity. In a particular embodiment, the one or more deterministic events correspond to an online event, and the online event includes one or more of a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier, a purchase or replacement of the communications device, a removal and/or replacement of a subscriber identity module, and a password reset of the communications device. In a particular embodiment, the method may additionally include revising the two or more nodes of the identity network to exclude the persistent identifier. In a particular embodiment, the method may additionally include grouping the two or more nodes and one or more additional nodes of the identity network into one or more relationship groups, the one or more relationship groups including a content group, a transactions group, a financial group, a family group, a household group, a group associated with a physical address of the subscriber, a social network group, and a merchant group. Implemen-

US 12,058,528 B2

3

tations of the described techniques may include hardware, a method or process, or computer software on a computer-accessible medium.

Another general embodiment may be directed to an apparatus that includes at least one processor coupled to at least one memory device to transmit a message to a communications device. The apparatus may additionally receive a signal, in response to the transmitted message, to verify that a subscriber having a real-world identity is co-located with the communications device. The apparatus may additionally establish, in an electronic or digital domain, two or more nodes of an identity network to correspond to aspects of the real-world identity of the subscriber, the identity network is to be attached to the real-world identity via a persistent identifier, and the two or more nodes of the identity network are to be linked via one or more relationships.

In particular embodiments, the persistent identifier includes a subscriber-unique alias. In particular embodiments, the at least one processor coupled to the at least one memory device are additionally to establish one or more additional nodes of the identity network responsive to an electronic determination of an aspect of the electronic or digital domain corresponding to the subscriber, in which the aspect includes one or more of an electronic mail address of the real-world identity, an internet protocol address of the real-world identity, a wireline telephone number of the real-world identity, an identifier of an ancillary device, an institutional account in the name of the real-world identity, a healthcare account, or a transaction account of the real-world identity. In particular embodiments, the at least one processor coupled to the at least one memory device are additionally to establish one or more additional relationships between or among the one or more nodes of the identity network responsive to one or more electronically determined events that occur with respect to the real-world identity. Particular embodiments may also include the one or more electronically determined events correspond to one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, the healthcare account, and/or the transaction account in the name of the real-world identity. In particular embodiments, the apparatus is additionally to assign a confidence score to the real-world identity in the electronic or digital domain. In particular embodiments, the apparatus is additionally to revise the confidence score based, at least in part, on the one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, and/or the transaction account in the name of the real-world identity. In particular embodiments, the apparatus is further to access a data store to detect one or more deterministic events in relation to historical norms with respect to the communications device corresponding to the real-world identity. In particular embodiments, the one or more deterministic events correspond to an online event. In particular embodiments, the online event includes one or more of a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier, a purchase or replacement of the communications device, a removal and/or replacement of a subscriber iden-

4

tity module, and a password reset of the communications device. Implementations of the described techniques may include hardware, a method or process, or computer software on a computer-accessible medium.

Another general embodiment may be directed to an article including a non-transitory storage medium having instructions stored thereon which, when executed by a special-purpose computing platform having processor coupled to at least one memory device are operable to transmit a message to a communications device and to receive a signal, in response to the transmitted message, to verify that a subscriber having a real-world identity is co-located with the communications device. The processor coupled to the at least one memory device may also establish, in an electronic or digital domain, two or more nodes of an identity network to correspond to aspects of the real-world identity of the subscriber, wherein the identity network is to be attached to the real-world identity via a persistent identifier, and the two or more nodes of the identity network are to be linked via one or more relationships.

In particular embodiments, the stored instructions may revise two or more nodes of the identity network to exclude the persistent identifier. In particular embodiments, the stored instructions are additionally to direct the at least one processor coupled to the at least one memory device to establish one or more additional nodes of the identity network responsive to an electronic determination of an aspect of the electronic or digital domain corresponding to the subscriber, in which the aspect may include one or more of: an electronic mail address of the real-world identity, an internet protocol address of the real-world identity, a wireline telephone number of the real-world identity, an identifier of an ancillary device, an institutional account in the name of the real-world identity, a healthcare account, or a transaction account of the real-world identity. In particular embodiments, the stored instructions are additionally to direct the at least one processor coupled to the at least one memory device to establish one or more additional relationships between or among the one or more nodes of the identity network responsive to one or more electronically determined events that occur with respect to the real-world identity. In particular embodiments, the one or more electronically determined events correspond to one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, the healthcare account, and/or the transaction account in the name of the real-world identity. In particular embodiments, the stored instructions are additionally to direct the at least one processor coupled to the at least one memory device to assign a confidence score to the real-world identity in the electronic or digital domain. In particular embodiments, the stored instructions are additionally to revise the confidence score based, at least in part, on the one or more interactions between the real-world identity and the electronic mail address of the real-world identity, the internet protocol address of the real-world identity, the wireline telephone number of the real-world identity, the identifier of the ancillary device, the institutional account of the real-world identity, and/or the transaction account in the name of the real-world identity. In particular embodiments, the stored instructions are additionally to direct the at least one processor coupled to the at least one memory device to access a data store to detect one or more deterministic events in relation to historical norms with respect to the commu-

US 12,058,528 B2

5

nications device corresponding to the real-world identity. In particular embodiments, the one or more deterministic events correspond to an online event. In particular embodiments, the online event includes one or more of a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier, a purchase or replacement of the communications device, a removal and/or replacement of a subscriber identity module (sim), and a password reset of the communications device.

BRIEF DESCRIPTION OF THE DRAWINGS

Claimed subject matter is particularly pointed out and distinctly claimed in the concluding portion of the specification. However, both as to organization and/or method of operation, together with objects, features, and/or advantages thereof, claimed subject matter may best be understood by reference to the following detailed description if read with the accompanying drawings in which:

FIG. 1 is a diagram illustrating features associated with an implementation of an example communications infrastructure, which may facilitate an identity verification platform to establish a tie between a subscriber's real-world and digital identity, according to an embodiment.

FIG. 2 is a diagram showing an implementation of an example use case or scenario for a subscriber to interact with an identity verification platform, according to an embodiment.

FIG. 3 is a diagram showing potential relationships between subscribers' real-world identities and the identities of such subscribers in an electronic or digital domain, according to an embodiment.

FIG. 4A is a diagram showing various ties between subscribers' real-world identities and the identities of such subscribers in an electronic or digital domain, according to an embodiment.

FIG. 4B is a diagram showing signal flow between a communications device, a merchant, and a verifying entity, according to an embodiment.

FIG. 5 is a diagram showing an identity network in an electronic or digital domain that is tied to a subscriber's real-world identity via a subscriber account identifier, according to an embodiment.

FIG. 6 is a diagram showing an identity network in an electronic or digital domain showing ties among various aspects of a subscriber's identity network, according to an embodiment.

FIG. 7 is a diagram showing changes in ties between or among aspects of a subscriber's identity network in an electronic or digital domain, according to an embodiment.

FIG. 8 is a diagram showing modifications to an identity network in an electronic or digital domain, according to an embodiment.

FIG. 9 is a diagram showing modifications to an identity network in an electronic or digital domain responsive to use of a one-time password, according to an embodiment.

FIG. 10 is a diagram showing a generalized identity network in an electronic or digital domain, according to an embodiment.

FIG. 11 are diagrams showing additional identity networks in an electronic or digital domain, according to an embodiment.

FIG. 12 is an identity network showing interactions to modify ties in a subscriber's identity and electronic digital domain, according to an embodiment.

6

FIG. 13 is a schematic diagram illustrating an implementation of a computing device in an example computing environment, according to an embodiment.

FIG. 14 is a flowchart for a method of representing electronically stored identity networks of a subscriber to a communication services carrier in an electronic or digital domain.

Reference is made in the following detailed description to accompanying drawings, which form a part hereof, wherein like numerals may designate like parts throughout that are corresponding and/or analogous. It will be appreciated that the figures have not necessarily been drawn to scale, such as for simplicity and/or clarity of illustration. For example, dimensions of some aspects may be exaggerated relative to others, one or more aspects, properties, etc. may be omitted, such as for ease of discussion, or the like. Further, it is to be understood that other embodiments may be utilized. Furthermore, structural and/or other changes may be made without departing from claimed subject matter. References throughout this specification to "claimed subject matter" refer to subject matter intended to be covered by one or more claims, or any portion thereof, and are not necessarily intended to refer to a complete claim set, to a particular combination of claim sets (e.g., method claims, apparatus claims, etc.), or to a particular claim. It should also be noted that directions and/or references, for example, such as up, down, top, bottom, and so on, may be used to facilitate discussion of drawings and are not intended to restrict application of claimed subject matter. Therefore, the following detailed description is not to be taken to limit claimed subject matter and/or equivalents.

DETAILED DESCRIPTION

References throughout this specification to one implementation, an implementation, one embodiment, an embodiment, and/or the like means that a particular feature, structure, characteristic, and/or the like described in relation to a particular implementation and/or embodiment is included in at least one implementation and/or embodiment of claimed subject matter. Thus, appearances of such phrases, for example, in various places throughout this specification are not necessarily intended to refer to the same implementation and/or embodiment or to any one particular implementation and/or embodiment. Furthermore, it is to be understood that particular features, structures, characteristics, or the like described are capable of being combined in various ways in one or more implementations and/or embodiments and, therefore, are within intended claim scope. In general, of course, for the specification of a patent application, these and other issues have a potential to vary in a particular context of usage. In other words, throughout the disclosure, particular context of description and/or usage provides helpful guidance regarding reasonable inferences to be drawn; however, likewise, "in this context" in general without further qualification refers at least to the context of the present patent application.

Some example methods, apparatuses, and/or articles of manufacture are disclosed herein that may be used, in whole or in part, to facilitate and/or support one or more operations and/or techniques for implementing an identity verification platform, such as via one or more computing and/or communication networks and/or protocols (e.g., network protocols) discussed herein. As will be seen, in some instances, operations and/or techniques for implementing an identity verification platform, may be implemented, at least in part, to authenticate and/or verify an identity and/or trustworthi-

US 12,058,528 B2

7

ness of a subscriber having an account, for example, with a mobile communication services provider.

In this context, an “account,” such as described hereinabove, may represent an aspect of a subscriber’s presence in an electronic or domain. Accordingly, in a manner similar to the manner in which a real-world subscriber may possess particular physical aspects, such as biometric aspects, which may include height, weight, hair color, eye color, parameters extracted from an image of a subscriber’s face (e.g., so as to facilitate facial recognition), a unique fingerprint or thumbprint, a unique walking stride or gait, a subscriber may possess aspects in an electronic or digital domain. For example, in an electronic or digital domain, a subscriber may possess aspects, such as a subscriber account identifier (e.g., mobile or landline telephone number), a persistent identifier or a subscriber-unique alias that associates or couples a subscriber to a communications device, one or more email addresses, one or more bank account numbers or identifiers with performing other types of transactions, healthcare records, one or more brokerage account numbers, a Social Security number, a username and password to obtain restricted or premium content, a media access control (MAC) address, an Internet protocol (IP) address, etc. It should be noted that claimed subject matter is intended to embrace any record that is assignable to a real-world entity, such as an individual subscriber or to a persona representing an individual subscriber.

As also discussed below, one or more operations and/or techniques for implementing an identity verification platform within an electronic infrastructure may permit a particular institution or organization, such as a bank to verify identity and/or trustworthiness of a user. Such verification may be achieved by utilizing sensitive content or data held by a particular data source, such as a communication services provider, a communications device (e.g., a mobile cellular telephone, and IOT device, a laptop computer), or the like. In addition, such identity verification may be achieved via accessing a data source that includes subscriber-specific parameters and/or identifiers such as subscriber names, subscriber physical addresses, social network groups of which a subscriber may be a member, subscriber employers, members of a subscriber’s family, members of a subscriber’s household, and a host of additional parameters and/or identifiers. In this context, “data source” refers to a source of content, which may include private consumer content, personally identifiable information, premium entertainment content, etc.

As alluded to previously, in a society in which electronic commerce, facilitated via communications devices (e.g. mobile communications devices), takes place on a grand scale, occurrences of fraud, unfortunately, are increasing in frequency and number. Such fraud may occur in connection with everyday transactions, which may include financial fraud, false transactions, theft of funds, purchases with stolen credit cards, and so forth. To reduce the likelihood of such fraud, various anti-fraud procedures may be implemented to preclude all types of fraud, which may include fraud associated with online transactions and/or in-store purchases involving all types of goods and/or services. Likewise, in a world in which various electronic devices typically used for communication, such as wireline telephones, mobile cellular telephones, tablets, laptop computers, etc., are ubiquitous, the types of possible fraud have, in at least some instances, become more complex. Occurrences of fraud may involve the use and/or knowledge of complex technology, for example, which may be related to the

8

particular hardware and/or software platforms associated with such cellular telephones, tablets, laptop computers, etc.

In other instances, fraud may occur via an electronic impersonation of a real-world identity (e.g., a fictitious subscriber) utilizing a “bot,” which refers to a computer-instantiated impersonated real-world entity. Additional instances of fraud may include reputational fraud, in which an entity posts false-negative or false-positive reviews on a popular review site, thus providing a source of misinformation that may be disseminated among large groups of people. In other instances, peer-to-peer fraud may occur, in which a “bot,” for example, may post fake positive or negative reviews on user review sites for service providers offering vehicles for hire, food delivery, package delivery, couriers, freight transportation, etc. In still other instances, fraud may occur by way of audience manipulation, such as an audience of a social network site, for example, by creating fake accounts, posing as a member of a social networking community, posting false accounts of incidents which may never have occurred, etc. Thus, for numerous reasons, ways to combat fraud, including, but not limited to the above-identified fraudulent behaviors that may occur online and/or electronically, continues to be an active area of investigation.

One approach toward reducing the risk of potential fraud relates to identity authentication and/or verification of a user, customer, subscriber, or purchaser, typically prior to completion of a transaction (e.g., in place of or in addition to) a typical log-in. In this context, the term “transaction” (or similar term) refers to a set of communications and/or actions that take place between at least two parties that reciprocally affect and/or influence the parties involved in the transaction. Entities that provide identity verification services are referred to herein as “identity verifiers,” identity verification services,” or utilizing similar terms. For example, an agent (e.g., a financial institution, a content provider, healthcare provider, and employment service, etc.) may include an entity that facilitates and/or supports an identity verification service. An agent may function to organize and/or participating in one or more transactions between two other parties (e.g., a bank and a telecommunication services carrier, etc.). In this context, it is to be understood that identity verification may be requested for a significant number of users for a corresponding number of possible situations. For example, millions, tens of millions, hundreds of millions or even more requests for identity verification may be submitted on a daily basis, for example. Therefore, it may be desirable to implement consistent and repeatable approaches and/or processes that can be utilized in connection with a large volume of identity verification requests, rather than uniquely customized approaches and/or processes that may vary on a request-by-request basis.

As will be discussed, identity verification is an possible approach to reduce the risk of fraud. Other approaches, such as approaches to authentication and/or verification may also be used herein, in whole or in part, such as a part of, in addition to, and/or in conjunction with identity verification. With respect to identity verification, in a worldwide electronic communications environment, a subscriber of a communication services carrier (e.g., a mobile communication services carrier) may establish an identity with such a carrier and/or with a third party. Such third parties may include, but are not limited to, an online merchant, who may be willing to interact with a user (e.g., customer, subscriber, purchaser, etc., to sell, extend services, provide access to content, etc.) if an identity is to be verified. In many instances, given the nature of certain transactions, especially in a communica-

US 12,058,528 B2

9

tions environment in which transactions take place via a communications network around the clock and at geographically dispersed locations, it may be useful to perform identity verification relatively quickly, such as in a real-time (or near real time) fashion.

As a general matter, authentication and/or verification of a subscriber (e.g., mobile subscriber) may be desirable in response to an institution or organization (e.g., third party, etc.) seeking to verify the identity of a user (e.g., mobile subscriber). In conventional approaches, identity verification tends to rely on authenticating or verifying an existing tie and/or association to a persistent mobile identifier, as demonstrated below through illustrative examples. In this context, the term “bind,” “association,” or similar terms, refer to a persistent, continuing and objectively verifiable relationship between a user (e.g., subscriber, person, entity, etc.) and an electronic or digital identity, including, as an example, a subscriber and a bank or other financial institution or organization holding or curating the subscriber’s bank account. Thus, a “subscriber account identifier,” “persistent identifier,” or “subscriber-unique alias,” may be employed to represent a real-world identity in an electronic or digital domain. In this context, the term “subscriber account identifier” refers to an identifier that relies on account relationship (also referred to as a tie and/or association) between a subscriber and a communication services carrier. In some instances, a “subscriber account identifier” refers to a mobile (or wireline) telephone number. On the other hand, a “persistent identifier” or a “subscriber-unique alias” refer to an identity that indicates a relationship between a subscriber and an identity verifier. Thus, responsive to a particular subscriber severing an account relationship with a first communication services carrier and establishing a relationship with a second communication services carrier, the second communication services carrier may electronically assign a new subscriber account identifier to the subscriber. However, throughout transitions between communication services carriers, an identity verifier may continue to identify and/or refer to the subscriber via a “persistent identifier” or a “subscriber-unique alias.”

Other aspects of subscriber authentication and/or verification are described herein. As noted, in an embodiment, verification, such as mobile subscriber identity verification, may relate to a mobile account and/or a mobile subscriber, for example. As mentioned, a mobile account is one example of a type of account, especially in an online world, although claimed subject matter is not intended to be limited to online accounts or to mobile accounts. Rather, the term “account” in this context refers to a formal business arrangement between an entity and/or person and a provider of the account in order to accomplish a business purpose. It is noted, for clarification, that in some situations, a person may represent an entity, for example. Likewise, in some situations, a person and an entity may be distinct. Further, the term account is to be read broadly and may include a service account, a financial account, an account relating to access to content, an account relating to one or more health care providers, an account relating to a government or administrative entity, just to name a few illustrative examples. Thus, continuing with non-limiting examples, an account identifier, in various embodiments, may, for example, be employed with respect to purchase of goods and/or services, access to content, access to financial accounts, access to medical records, access to corporate or organizational intellectual property and/or other types of records and/or files, access to other services, etc. in this context, an account identifier refers to a user-assigned or entity-assigned com-

10

bination of one or more alphanumeric terms or other symbols, which allows access to a system or to content in an electronic digital domain.

In addition to a subscriber account identifier, a persistent identifier, and a subscriber-unique alias referring to a particular communications device, such terms may additionally refer to a particular communications device. Such communication devices may also be identified via a telephone number (e.g., a mobile telephone number), an international mobile subscriber identifier (IMSI), Integrated Circuit Card Identifier (ICC ID), and/or other type of identifier (e.g., a unique identifier) employed in connection with the particular mobile network operator or the mobile communication services provider. Mobile communications networks may include those compatible or compliant with a Global System for Mobile Communications (GSM) telecommunications network, for example. Other examples of mobile subscriber account identifiers may include an international mobile equipment identifier (IMEI), a mobile equipment identifier or any other identifier including a mobile billing account number or identifier.

Although the discussion that follows relates to any type of account, as a non-limiting illustration, mobile accounts are used for illustration. It is understood, of course, that claimed subject matter is intended to not be limited to examples provided primarily for purposes of illustration, since such examples may be oversimplified for purposes of comprehension, for example. As was mentioned previously, with respect to commerce, including, of course, mobile accounts, a risk of fraud and/or unauthorized actions taking place is present or at least a risk exists of attempts being made.

The following provides a few illustrative examples of accounts in which a risk of fraud and/or unauthorized actions may be present. In scenarios, user may log into a bank account via a web browser or an executable application on a communications device (e.g., a mobile communications device), for example. In response to receipt of signals initiated by the user, a financial institution, for example, may utilize an application programming interface (API) substantially compatible and/or substantially compliant with HTTP and/or HTTPS, including versions now known and/or to be later developed, and/or another suitable protocol (e.g., now known and/or to later be developed). In such an example, a user may seek to take one or more actions with respect to an account, for example, to transfer funds, view a history of transactions, make a payment, update sensitive content, access or update subscriber-specific parameters, etc. In another illustration, a mobile communication services subscriber may seek to access an existing account with a merchant. In response, a merchant, such as a provider of online music or other provider of entertainment-related content, may seek a form of payment, such as via a credit account (e.g., credit card) that may already be on record with the merchant. In another illustration, a user may seek to access a communications device, for example, to create, share, and/or edit a file.

Thus, as suggested, a communication services subscriber (e.g., a mobile communication services subscriber) may seek to access, for example, an online account. A third party, such as those who may provide access to such an accounts, may seek to provide access control so as to restrict access to sensitive content. In an example, a software company and/or product, such as a developer of tax-preparation software products, may permit subscriber (access controlled) user accounts to be established. In another instance, a user may desire to access content, such as content corresponding to sensitive content (e.g., provided by a user to a social media

US 12,058,528 B2

11

account). In another instance, a user may return to a website and/or application, in which access to the website could be dependent, at least partially, on binding a user to a website and/or with an application, such as via an subscriber account identifier for the user. Thus, a third party may comprise a customer care facility of an enterprise, for example, such as a customer-care facility of a bank, in which an account is established and/or maintained.

As previously mentioned herein, authenticating and/or verifying a subscriber of a communications device may be instrumental in reducing the risk of fraudulent behavior, such as credit card fraud, wire fraud, bank fraud, and so forth. To increase the likelihood that a legitimate, bona fide mobile subscriber can complete a transaction (e.g., a financial transaction, a transaction to obtain fee-based content, or other type of transaction), an identity verifier may query one or more databases. Parameters obtained from the one or more databases may be utilized to complement parameters supplied by, for example, the mobile subscriber, and/or a communications device. In particular embodiments, a communications device may store physical parameters of a subscriber, such as subscriber-specific biometric aspects, which may include height, weight, hair color, eye color, parameters extracted from an image of a subscriber's face (e.g., so as to facilitate facial recognition), a unique fingerprint or thumbprint, a unique walking stride or gait, etc. Subscriber-specific physical parameters may be stored in a protected memory area of a subscriber's communications device, which may facilitate identification of the subscriber. Identity of a subscriber, obtained via accessing a protected area of the communications device may be utilized to generate a tokenized digital signature. In particular embodiments, a tokenized digital signature may facilitate completion of an authentication process initiated by an identity verifier in response to an authentication request generated by a merchant, financial institution, premium content provider, or the like.

It should be noted, however, that in many instances, databases utilized by identity verifiers and/or authenticators may be only partially complete. Accordingly, in some instances, authenticating and/or verifying the identity of a mobile subscriber may be successful in only a limited number of circumstances. Such limited success in authenticating and/or verifying an identity of a mobile subscriber may be attributed, at least in part, to use of imprecise (e.g., "fuzzy") logic. Utilizing fuzzy logic, minor inconsistencies between subscriber parameters may be ignored, so long as, on balance, such subscriber parameters are likely to correspond to a particular subscriber. In one possible example just for the sake of illustration, a first subscriber named John Smith, living in New York City, may be confused with Jonathan Smith, living in a suburb of New York City. In another possible example, two or more parameters, considered in the aggregate, may bring about confusion and/or ambiguity in authentication and/or verification of a subscriber. For example, a first subscriber named John Smith, having a physical address in New York City, and having a Social Security number of 556-55-5555 may be confused with John Smyth, also having a physical address in New York City, and having a Social Security number of 555-55-5555. In such instances, wherein distinct subscribers in the real world may be confused with one another, permitting such subscribers to engage in transactions, such as financial transactions, may be indicative of an opportunity to engage in fraudulent behavior. For example, an unscrupulous individual, may attempt to impersonate a particular subscriber, such as by obtaining a phone number having digits that are

12

similar to those of the subscriber, obtaining an electronic mail address that is similar to an electronic mail address of another subscriber, and so forth.

As mentioned previously, one approach toward mitigation of the risk of fraud may be to employ authentication and/or verification, which may include a tie identity authentication or verification of trustworthiness of a communication services subscriber. In particular embodiments, as will be described herein, an identity verification platform may permit an institution or organization, such as a financial institution, to verify identity and/or trustworthiness of a user by using sensitive content (e.g., personally identifiable information) held by a particular data source. Authentication and/or verification of a subscriber (e.g., a mobile subscriber) may operate to form a tie between the subscriber, which may be represented in an electronic or digital domain. Such a tie may indicate the presence of a relatively strong bond or relationship between the identity of a real-world subscriber and the digital identity of such subscriber (in an electronic or digital domain).

Such a tie between a real-world subscriber and a digital identity of such subscriber in an electronic or digital domain may be relatively strong since many subscribers find it difficult to participate in contemporary society in the absence of certain types of communications devices, such as communications devices. For example, in many instances, certain types of communications devices, such as mobile communications devices, provide not only voice/data communications capabilities, but may also provide location services, calendaring services, entertainment, gaming, social networking, as selected by the subscriber. Accordingly, in contrast to the loss of a particular credit card, a driver's license, or a passport, for example, which may go unnoticed for a period of days or even weeks, loss of a communications device may be noticed immediately, perhaps within minutes or even seconds of misplacement or loss of device. Hence, it may be appreciated that if an subscriber misplaces a communications device, such a subscriber may rapidly attempt to recover the device, or may replace the device immediately.

Accordingly, certain types of communication devices may be instrumental in providing a tie between a real-world subscriber and a digital identity of such a subscriber (e.g., in an electronic or digital domain). Further in view of the importance that many subscribers place on personal mobile communications devices, establishing a tie between an subscriber's real-world identity and such a communications device may tie the identity of a real-world subscriber to an electronic or digital identity of such subscriber. For example, in an electronic or digital domain, a subscriber account identifier (e.g., a mobile telephone number) may be tied to a particular email address, such as an email address to which invoices for communication services may be conveyed. Accordingly, upon establishing a relationship between a real-world subscriber and a digital identity, such as by way of tying a real-world subscriber with a subscriber account number in an electronic or digital domain, additional aspects of the subscriber's digital identity may be constructed. Thus, in one possible example, following the electronic determination of a tie between a real-world subscriber and a subscriber account identifier as well as an email address, an Internet protocol (IP) address to which such emails may be delivered may also be ascertained. Thus, it may be appreciated that the tie between a real-world subscriber and a digital identity of such an subscriber may serve as a conduit, which can be exploited to construct or form additional aspects the subscriber's digital identity may be constructed.

US 12,058,528 B2

13

In particular embodiments, such exploitation of a conduit formed between an subscriber's real-world identity and the subscriber's digital identity, utilizing a subscriber account identifier (e.g., a mobile telephone number) may be facilitated utilizing an identity verification platform. In particular

embodiments, an identity verification platform may operate within a communications infrastructure, such as shown in FIG. 1. FIG. 1 is a diagram illustrating features associated with an implementation of an example communications infrastructure, which may facilitate an identity verification platform to establish a tie between a subscriber's real-world and digital identity, according to an embodiment. Processes and/or operations for an identity verification platform may be implemented, at least in part, to validate identity of a communications services subscriber utilizing, for example, a communications device referenced herein at **102**. As used herein, "communications device" may refer to any kind of special purpose computing platform and/or apparatus that may, at least under particular circumstances, occupy a position or location that changes from time to time. As a way of illustration, communications devices, such as mobile communications devices including, for example, wireline telephones, cellular telephones, smart telephones, laptop computers, personal entertainment systems, tablet personal computers (PC), personal audio or video devices, personal navigation devices, Internet of Things (IoT) devices, or the like. It should be noted, however, that these are merely examples of communications devices that may be used, at least in part, to implement one or more operations and/or techniques for implementing an utilizing identity verification platform, and that claimed subject matter is not limited in this respect.

It should be appreciated that operating a communications infrastructure **100** is described herein as a non-limiting example that may be implemented, in whole or in part, in the context of various electronic communications networks or combination of such networks, such as public networks (e.g., the Internet, the World Wide Web), private networks (e.g., intranets), WWAN, wireless local area networks (WLAN, etc.), or the like. It should also be noted that claimed subject matter is not limited to a particular network and/or operating environment. For example, in some instances, an optical network may be used herein, in whole or in part, such as separately and/or in any suitable combination with one or more networks discussed herein. Thus, depending on an implementation, one or more operations and/or techniques for implementing an identity verification platform.

In an implementation, communications device **102** may, for example, receive or acquire satellite positioning system (SPS) signals **104** from SPS satellites **106**. In some instances, SPS satellites **106** may be from a single global navigation satellite system (GNSS), such as the GPS or Galileo satellite systems, for example. In other instances, SPS satellites **106** may be from multiple GNSS such as, but not limited to, GPS, Galileo, Glonass, or Beidou (Compass) satellite systems. In certain implementations, SPS satellites **106** may be from any one several regional navigation satellite systems (RNSS) such as, for example, WAAS, EGNOS, QZSS, just to name a few examples.

At times, communications device **102** may, for example, transmit wireless signals to, or receive wireless signals from, a wireless communication network. In one example, communications device **102** may communicate with a cellular communication network, such as by transmitting wireless signals to, or receiving wireless signals from, one or more

14

wireless transmitters capable of transmitting and/or receiving wireless signals, such as a base station transceiver **108** over a wireless communication link **110**, for example. Similarly, communications device **102** may transmit wireless signals to, or receive wireless signals from a local transceiver **112** over a wireless communication link **114**. Base station transceiver **108**, local transceiver **112**, etc. may be of the same or similar type, for example, or may represent different types of devices, such as access points, radio beacons, cellular base stations, femtocells, or the like, depending on an implementation. Similarly, local transceiver **112** may comprise, for example, a wireless transmitter and/or receiver capable of transmitting and/or receiving wireless signals. For example, as will be seen, at times, wireless transceiver **112** may be capable of obtaining one or more observations from one or more other terrestrial transmitters.

In a particular implementation, local transceiver **112** may communicate with communications device **102** at a shorter range over wireless communication link **114** than at a range established via base station transceiver **108** over wireless communication link **110**. For example, local transceiver **112** may be positioned in an indoor or like environment and may provide access to a wireless local area network (WLAN, e.g., IEEE Std. 802.11 network, etc.) or wireless personal area network (WPAN, e.g., Bluetooth® network, etc.). In another example implementation, local transceiver **112** may comprise a femtocell or picocell capable of facilitating communication via link **114** according to an applicable cellular or like wireless communication protocol. It should be understood that these are merely examples of networks that may communicate with communications device **102** over a wireless link, and claimed subject matter is not limited in this respect. For example, in some instances, communications infrastructure **100** may include a larger number of base station transceivers **108**, local transceivers **112**, etc.

In an implementation, base station transceiver **108** and local transceiver **112** may communicate with server **116** over a network **122** via one or more links **124**. Network **122** may comprise, for example, combinations of wired or wireless communication links. In a particular implementation, network **122** may comprise, for example, a network capable of implementing an Internet Protocol (IP) infrastructure capable of facilitating or supporting communication between communications device **102** and server **116** via local transceiver **112**, base station transceiver **108**, etc. In another implementation, network **122** may comprise, for example cellular communication network infrastructure, such as a base station controller or master switching center to facilitate and/or support, for example, mobile cellular communication with communications device **102**. Server **116** may comprise one or more database servers (e.g., for a data source, agent, identity verifier, communication services carrier, etc.), update servers, back-end servers, management servers, archive servers, location servers, positioning assistance servers, navigation servers, map servers, crowdsourcing servers, network-related servers, or the like.

In particular implementations, communications device **102** may comprise circuitry and/or processing resources capable of determining a position fix or estimated location of communications device **102**, initial (e.g., a priori) or otherwise. For example, if satellite signals **104** are available, communications device **102** may compute a position fix based, at least in part, on pseudorange measurements to four or more SPS satellites **106**. Here, communications device **102** may compute such pseudorange measurements based, at

US 12,058,528 B2

15

least in part, on pseudonoise code phase detections in signals **104** acquired from four or more SPS satellites **106**. In particular implementations, communications device **102** may receive from one or more of servers **116** positioning assistance data to aid in the acquisition of signals **104** transmitted by SPS satellites **106** including, for example, almanac, ephemeris data, Doppler search windows, just to name a few examples.

Even though a certain number of computing platforms and/or devices are illustrated herein, any number of suitable computing platforms and/or devices may be implemented to facilitate and/or support one or more techniques and/or processes associated with communications infrastructure **100**. For example, at times, network **122** may be coupled to one or more wired or wireless communication networks (e.g., WLAN, etc.) so as to enhance a coverage area for communications with communications device **102**, one or more base station transceivers **108**, local transceiver **112**, server **116**, or the like. In some instances, network **122** may facilitate and/or support femtocell-based operative regions of coverage, for example. Again, these are merely example implementations, and claimed subject matter is not limited in this regard.

Thus, one or more operations and/or techniques for establishing a tie or an attachment between the identity of a real-world subscriber with the digital identity of such subscriber (in an electronic digital domain). Establishment of such a tie or other type of attachment may allow an institution or organization (e.g., a financial institution, etc.) to authenticate and/or verify identity of, for example, a subscriber to a mobile communication services provider. Such a tie or other type of attachment may additionally permit assessment of the trustworthiness of a subscriber utilizing records of deterministic online events with respect to a communications device in possession of (or co-located with) a communication services subscriber. Such a tie or attachment between real-world and digital identities of a subscriber may operate to ensure that sensitive content, such as a subscriber's personally identifiable information, usernames and/or passwords, account numbers, health records, confidential employment records, etc., does not become exposed to unscrupulous individuals.

Attention is now drawn to FIG. 2, which is a diagram showing an implementation of an example use case or scenario for a subscriber to interact with an identity verification platform, according to an embodiment **200**. In FIG. 2, subscriber **205** is co-located with communications device **102**. The embodiment of FIG. 2 may be implemented utilizing an identity verification platform **232**, which may comprise virtual or physical computing resources (e.g., computing devices) or any combination thereof. Identity verification platform **232** may execute computer-readable instructions (e.g., software, firmware, etc.), so as to implement one or more operations and/or processes, as discussed herein. In embodiment **200**, identity verification platform **232** may be deployed, such as being physically located, for example, so as to be directed by or under the control of identity verifier **230**. Responsive to determining that subscriber **205** has connected to a particular uniform resource locator (URL) via communications device **102**, identity verifier **230** may operate to establish a tie or other type of attachment between subscriber **205** and a digital identity of the subscriber. Such a tie or attachment may be established responsive to determining proof of possession of communications device **102**, determining that communications

16

device **102** is bound to a specific digital account assigned to subscriber **205**, and determining a reputation of communication device **102**.

Identity verifier **230** may implement one or more identity verification processes in real-time or in near-real time. In this context, "real-time" refers to an amount of timeliness of content, which may be delayed by an amount of time attributable to electronic communications involving a communications network and/or signal processing of any received signals. It should be noted that information acquired or produced, for example, by input signals, output signals, operations, results, etc., associated with embodiment **200** may be represented via one or more digital signals. It should also be appreciated that even though one or more operations are illustrated or described concurrently or with respect to a certain sequence, other sequences or concurrent operations may be employed. In addition, although the description below references particular aspects or features illustrated in certain other figures, one or more operations may be performed with other aspects or features. For example, in some instances, embodiment **200** may be implemented, in whole or in part, within the communications infrastructure of FIG. 1.

Thus, embodiment **200** may, for example, begin with subscriber **205** of a communication services carrier interacting with communications device **102**. Communications device **102** may interact with identity verifier **230** via a communications link, such as link **110**, perhaps via a cellular transceiver, such as base station transceiver **108** of FIG. 1. Identity verifier **230** may access subscriber parameters, such as a subscriber account identifier, subscriber name, and subscriber address, for example, from authentication and/or verification data store **234**. In some instances, identity verification platform **232** may provide data store **234** with, exclusively, utilizing a telephone number of (e.g., a mobile telephone number) obtained from communications device **102** received via communications link **110**.

In particular embodiments, an identity verification platform may obtain a persistent identifier and/or a subscriber-unique alias from subscriber **205**, which may function as an identifier that is more persistent than other types of identifiers, such as, for example, a mobile telephone number or other type of subscriber account identifier. In such embodiments, an identity verification platform may assign a persistent identifier to a subscriber so that, for example, even if a subscriber obtains a telephone number (e.g., a mobile telephone number) the persistent identifier may remain unchanged. In particular embodiments, a persistent identifier may persist even after service-disconnection, service-suspension events, switching from a first communication services carrier to a second communication services carrier, removal/replacement of a subscriber identity module, and so forth, may nonetheless persist.

In other embodiments, identity verification platform **232** may receive, via communications link **110**, a subscriber account identifier, a persistent identifier, a subscriber-unique alias, or other identifier separate from a telephone number. An additional identifier may comprise an international mobile subscriber identifier (IMSI), an international mobile electronic identifier (IMEI), or a mobile station international subscriber directory number (MSISDN), or any combination thereof. In turn, an application program interface (API) of data store **234** may match a provided subscriber account identifier with parameters of a particular subscriber, such as name, physical address, current employer, etc. perhaps by accessing internal communication services records, for example.

US 12,058,528 B2

17

In the embodiment of FIG. 2, identity verifier 230 may determine or ascertain proof of possession of communications device 102 by subscriber 205. Thus, for example, identity verifier 230 may convey a text, or other type of short message to communications device 102, along with a prompt, which may request that subscriber 205 enter the text or other type of short message into a user interface of communications device 102. As such, identity verifier 230 may verify that subscriber 205 is, indeed, in possession of communications device 102. Identity verifier 230 may additionally convey a second parameter to communications device 102, so as to determine the identity of subscriber 205 and/or to determine if subscriber 205 possesses an account relationship with a communication services carrier providing services to device 102. In one possible example, identity verifier 230 may request that a particular parameter not generally known to individuals other than subscriber 205 be entered into a user interface of communications device 102. In a possible example, subscriber 205 may be prompted to enter the last four digits of a Social Security number, a mother's maiden name, or may be requested to answer some other type of query with the response that, again, is not generally known to individuals other than subscriber 205.

In response to determining that subscriber 205 is in possession of communications device 102 and in response to determining that subscriber 205 has entered into an agreement (e.g., a bind or contract) with a communication services carrier providing such services to device 102, identity verifier 230 may additionally electronically determine a reputation of subscriber 205 with respect to communications device 102. For example, identity verification platform 232 may determine such reputation based, at least in part, on records of deterministic online events involving communications device 102. Such records may relate, for example, to whether subscriber 205 has recently ported or reassigned a subscriber account identifier (e.g., telephone number) from a first communication services carrier to a second communication services carrier. In particular embodiments, a subscriber who has recently ported or reassigned a subscriber account identifier may be considered to have a compromised reputation, while a subscriber who has never ported, or has not ported a subscriber account identifier for an extended period of time, for example, may be considered to have a superior reputation. In particular embodiments, a subscriber who has maintained ownership of communications device 102 for only a short period of time (e.g., a tenure of less than six months for example) may be considered to have a compromised reputation, while a subscriber who retains ownership of a communications device for a long period of time (e.g., a tenure of more than two years) may be considered to have a superior reputation. In particular embodiments, a subscriber who has recently removed/replaced a SIM of communications device 102 may be considered to have a compromised reputation, while a subscriber who has never removed/replaced a SIM of device 102 may be considered to have a superior reputation. In particular embodiments, a subscriber who has recently reset a password that controls access to a subscriber account may be considered to have a compromised reputation. Claimed subject matter may embrace additional behaviors of subscriber 205 comprising various online events involving communications device 102, which, in this context, are referred to as "online" behaviors, virtually without limitation.

In addition to online behaviors, which refer to behaviors of subscriber 205 with respect to communications device 102, identity verifier 230 may utilize off-line behaviors to

18

determine a reputation of subscriber 205 with respect to device 102. Deterministic online events relating to off-line behaviors may refer to events undertaken by a subscriber that do not directly involve communications device 102. For example, a subscriber receiving a traffic citation (e.g., for unsafe speed, unsafe lane change, etc.) may represent a deterministic off-line event. In another example, a deterministic off-line event may refer to a subscriber having a record of voting in at least some (or perhaps all) recent city, county, state, and/or federal elections. In another example, a deterministic off-line event may refer to a subscriber obtaining a library card, becoming a member of a local service club, obtaining a gym or fitness center subscription, obtaining a security clearance from a government agency, having favorable employment history, and so forth, and claimed subject matter is not limited in this respect. Accordingly, off-line events undertaken by a subscriber that may be representative of risky behavior may bring about a compromised reputation, while more reputable behaviors may give rise to a superior reputation of subscriber 205 with respect to device 102.

It should be noted that in some instances, identity verifier 230 may consider behavioral, historical norms with respect to both online and off-line behaviors. For example, a mobile subscriber who tends to (historically, such as over a 10-year period) port his or her phone at least once a year, may be assigned a superior reputation in response to the subscriber porting his or her phone twice within the most recent two-year period. However, a mobile subscriber who has never ported his or her mobile device, may be assigned a compromised reputation in response to the subscriber porting his or her phone twice within the same two-year period.

FIG. 3 is a diagram showing potential relationships between subscribers' real-world identities and the identities of such subscribers in an electronic or digital domain, according to an embodiment. As shown in FIG. 3, real-world entity John A. Smith (305A), Jacob Smith (305B), Judy Smith (305C), and Jane Smith (305D) may, perhaps, be associated with one or more email addresses or other aspects of the subscriber's electronic or digital domain. Thus, determining whether any of email addresses jsmith123@gmail.com, JS@hotdog_157.com, jsmith45@aol.com, soccermom@instagram.com are affiliated with John A. Smith (305A), Jacob Smith (305B), Judy Smith (305C), or Jane Smith (305D) can be problematic. Further, it should be noted that the above-identified email addresses include very little, if any, information that could be correlated with a particular subscriber's actual (real-world) name. For example, the email address jsmith123@gmail.com may (or may not) correspond to John Smith, Jacob Smith, Judy Smith, Jane Smith, or any one of hundreds or even thousands of individuals (including those for whom the name "Smith" does not form any part of that person's real-world identity).

FIG. 4A is a diagram showing various ties between subscribers' real-world identities and the identities of such subscribers in an electronic or digital domain, according to an embodiment 400. In the embodiment of FIG. 4A, for example, real-world entity (e.g., a subscriber) John Smith (305A) may be tied or bound to the subscriber account identifier (e.g., telephone number 303-555-1212), perhaps by way of authentication via identity verifier 230, as described in FIG. 2. Accordingly, following authentication and/or verification, which may involve electronically determining proof of possession of a communications device by John Smith, electronically determining that the communications device is bound to a specific digital account, and

US 12,058,528 B2

19

electronically determining a favorable reputation of the communications device, a tie may be established between the subscriber “John Smith” and identifier **410**, which may correspond to the subscriber account number 303-555-1212. It should be noted that a tie may also be established between a subscriber and any other type of subscriber account number (e.g., IMSI, ICC ID, MSISDN, etc.). Additionally, in particular embodiments, a tie may be established between the real-world subscriber “John Smith” and a persistent identifier as well as a subscriber-unique alias, and claimed subject matter is not limited in this respect.

In response to a tie existing between real-world entity John Smith (a subscriber) and subscriber account identifier 303-555-1212 (or any type of persistent identifier or subscriber-unique alias), it may be appreciated that additional aspects of the subscriber’s digital identity may be constructed. Accordingly, utilizing the subscriber account identifier as a conduit (e.g., a telephone number of 303-555-1212, such as indicated at **405A**), the email address jsmith123@gmail.com may be tied or bound (e.g., indirectly) to the real-world entity John Smith. Similarly, it may be appreciated that any number of additional email addresses belonging to John Smith (e.g., jsmithwork@gmail.com), a physical address of John Smith, an employer of John Smith, a driver’s license number, or any other parameter stored by (or accessible to) an identity verifier, such as identity verifier **230** of FIG. 2, may be utilized to construct additional aspects of John Smith’s digital identity in an electronic or digital domain. FIG. 4A additionally shows mapping of digital identities of Jane Smith (**305B**), Jacob Smith (**305C**), Judy Smith (**305D**) with @hotdog_157, jsmith45@aol.com, and soccermom@instagram.com, respectively. Mapping of digital identities is facilitated through subscriber account identifier **405B** (719-555-0123) subscriber account identifier **405C** (920-555-0073), and **405D** (414-555-0181), respectively.

Although not explicitly identified in FIG. 4A, a trustworthiness score or trustworthiness measure for a subscriber account identifier, a persistent identifier, and/or a subscriber-unique alias may be developed utilizing additional intelligence layers for associated identifiers and devices. For example, in addition to utilizing associations between, for example, an authenticated real-world entity and a communications device to determine additional aspects of a digital identity, probabilistic methods can be employed utilizing, for example, cross-device networks. Such networks may, for example, use a Mobile Advertising identification, a Wi-Fi IP address to associate devices, a subscription to a Virtual Private Network (VPN) to enhance links between aspects of a digital identity. In another example, geolocation may be utilized to increase confidence that a real-world identity is (indeed) in contact with an IP address known (or at least suspected) to be operating proximate (e.g., less than 0.5 km) to the geolocation of the real-world entity. In another example, if a real-world identity can be located within a particular ZIP Code, and such as ZIP Code is known to envelop certain IP addresses, confidence that the real-world identity is (indeed) communicating with the IP address can be enhanced. In other instances, a trustworthiness score or a trustworthiness measure may be enhanced utilizing data that suggests a real-world identity is within the same household (e.g. street address) of other, perhaps authenticated real-world identities. In some instances, determining that members of the household utilize the same or similar IP address may bring about such increases in trustworthiness score/measures.

20

In other instances, determining that a real-world entity interacts with a reputable financial institution, such as a large bank or brokerage firm, may bring about an increase in a trustworthiness score or measure. On the other hand, in other instances, determining that a real-world entity interacts with a less-reputable institution may bring about a lowering of a trustworthiness score or measure. In other instances, records from third-party identity-verification entities, such as a state or county government issuing a driver’s license to a real-world entity, issuance of a passport to a real-world subscriber, or any other regulated industry requiring, for example, credit checks, may enhance a trustworthiness score or measure.

FIG. 4B is a diagram showing signal flow between a mobile device, a merchant, and a verifying entity, according to an embodiment **450**. In the embodiment of FIG. 4B, a mobile communications device (e.g., communications device **102**) may engage or interact with merchant **460**. Such interaction may be to purchase, for example, a product or service, either remotely or in person, such as at a brick-and-mortar establishment. In response, merchant **460** may seek to authenticate and/or verify the mobile communications device. For example, merchant **460** may request the mobile phone number of the communications device, or may request any other identifier (e.g., a persistent identifier and/or a subscriber-unique alias) so as to obtain a measure of the creditworthiness of the subscriber. In turn, the merchant may interact with a verifier (e.g., identity verifier **230**). Responsive to verification of the communications device in possession of the subscriber, the verifier may indicate such verification to the communications device. Following verification of the communications device, the verifier may form or create a tie or other type of attachment between the communications device and the merchant. Such a tie or other type of attachment may be indicated via merchant-assigned identifier **480**, such as via an email address assigned to the mobile device by merchant **460**. In particular embodiments, the tie or attachment between the mobile device and the merchant (in an electronic or digital domain) may be attached (or appended) to the subscriber account identity (e.g., also in electronic or digital domain) corresponding to real-world identity **490**.

FIG. 5 is a diagram showing an identity network in an electronic or digital domain that is tied to a subscriber’s real-world identity via a subscriber account identifier, according to an embodiment **500**. FIG. 5 shows a relationship among the subscriber account identifier (e.g., a mobile telephone number), which forms a tie between the subscriber’s real-world identity and the subscriber’s identity in a digital or electronic domain. It should be noted, however, that in other embodiments, a persistent identifier or a subscriber-unique alias may be utilized to form a tie between the subscriber’s real-world identity and the subscriber’s identity in a digital or electronic domain. Thus, in FIG. 5, the subscriber’s communications device is first utilized to form the tie between the device from the real-world identity of a subscriber (e.g., a mobile subscriber) to an electronic or digital domain. Following such formation of a tie or link between the real-world and the electronic or digital domain, interactions between a real-world identity and various logical entities, such as the subscriber’s email addresses, can be utilized to gain insights with respect to the various online behaviors of the real-world identity as such behaviors reflect into the digital or electronic domain. In the example of FIG. 5, electronically determined event related to the subscriber account identifier 1-303-555-1212 and email address **510** (JSmith957@gmail.com) provides a tie between such email

US 12,058,528 B2

21

address, utilizing Gmail as the provider, and the subscriber account identifier. Likewise, electronically determining an event between the real-world identity corresponding to 1-303-555-1212 and twitter handle **310B** (JS@hotdog_157) indicates formation of a tie between the subscriber account identifier 1-303-555-1212 and twitter.com.

Thus, it may be appreciated that interactions between a real-world identity (e.g., a user, mobile subscriber, persona) and an aspect of an electronic or digital domain, such as a real-world identity interacting with an email address, a social network account, twitter account, or any other interaction among numerous possible interactions by way of a communications device, may permit strengthening of ties between a node (representing an aspect) of an identity network. Such strengthened ties may enhance trustworthiness of a real-world identity. For example, if a link between a real-world subscriber and the email address jsmith456@gmail.com is determined to be merely a tenuous or unverified link, successive interactions may boost or strengthen the link between the real-world subscriber and jsmith456@gmail.com. Such strengthening of links in an electronic or digital domain may enhance trustworthiness of a real-world identity. On the other hand, if a real-world identity regularly (e.g. in accordance with a historical norm) interacts with various aspects of an electronic or digital domain (e.g., accesses email, social networks, etc. on a regular basis, such as more than five per day) and then refrains from doing so for an extended period of time (e.g., accesses email and/or social network accounts less than once per week) such absences may degrade the link between the digital identity of the subscriber and, for example, jsmith456@gmail.com. Such degradations may negatively impact the trustworthiness of the real-world subscriber corresponding to the digital identity. Accordingly, it may be appreciated that a subscriber's trustworthiness may fluctuate in real-time (or in near-real-time), such as to occasionally increase in value and decrease in value, in response to the subscriber interactions with aspects of the identity network in a digital domain. Such fluctuation in real-time trustworthiness of a real-world identity may range in graduated levels that may range from a real-world entity being completely (or virtually) unverified/unauthenticated to a real-world identity being completely verified/authenticated. In some instances, a real-world identity corresponding to a subscriber may undergo large and nearly instantaneous degradations in trustworthiness, perhaps in response to the subscriber visiting websites or interacting with devices, known to be utilized for transmission of, for example, malware or utilized for engaging in other types of potentially dangerous behavior.

FIG. 6 is a diagram showing an identity network in an electronic or digital domain showing ties among various aspects of a subscriber's identity network, according to an embodiment **600**. In the embodiment of FIG. 6, which involves attempting to match email address **510** of a subscriber in an electronic or digital domain (jsmith957@gmail.com) with a real-world identity, such as subscriber **305A** (John Smith), subscriber **305C** (Judy Smith), subscriber **605** (Jackson S. Mith), may employ fuzzy or imprecise logic which may, for example, lead to potential possibilities for matching among real-world identities and, for example, an email address. Accordingly, although it may be possible to determine name and address, of an subscriber, such as John Smith living at address **610** (e.g., 123 Main Street, Columbus, Ohio), Judy Smith living at address **615** (e.g., 245 Second Street, Los Angeles Calif.), and Jackson S. Mith living at address **620** (e.g., 8115, Madeup Boulevard,

22

New Holstein Wisc.), such probability-based approaches may rarely result in an accurate match being electronically determined between a real-world entity and an email aspect of a digital identity in a digital or electronic domain. In some instances, attempting to match twitter handle **310B** (e.g., JS@hotdog_157), may be impossible or virtually impossible.

FIG. 7 is a diagram showing changes in ties between or among aspects of a subscriber's identity network in an electronic or digital domain, according to an embodiment **700**. As shown in FIG. 7, responsive to verification of proof-of-possession of a device, such as communications device **102** co-located with subscriber **205**, ties or other attachments among aspects of a digital identity in an electronic or digital domain may result in increased confidence in ascertaining aspects of a subscriber's electronic or digital domain. For example, responsive to verification of the position of a communications device by a particular subscriber, such as by way of establishing a tie between the subscriber account identifier (e.g., 1-303-5551212) and real-world identity John Smith, correctly identifying additional ties in an electronic or digital domain may be possible.

Hence, as shown in FIG. 7, responsive to a real-world identity of subscriber **305A** (John Smith) being verifiably in possession of, or co-located with, a particular communications device (e.g., a communications device corresponding to a specific subscriber account identifier, telephone number, persistent identifier, subscriber-unique alias, etc.), further interactions involving the communications device can authoritatively establish links between the real-world identity and email providers. For example, following electronic determination of a particular communications device accessing email address **510** (jsmith957@gmail.com), it may be straightforward to recognize that the real-world identity for subscriber **305A** (John Smith) can be linked with email provider **705** (Google.com) via such email address. Email provider **705** may correspond to digital identity **805**, which is an aspect of subscriber **305** a in an electronic or digital domain. In another example, following the electronic determination of a particular communications device accessing the twitter feed utilizing twitter handle **310B** (JS@hotdog_157), it may be straightforward to recognize that the real-world identity for subscriber **305A** (John Smith) can be linked with twitter.com via the JS@hotdog_157 handle. As a consequence of the formation of authoritative links among aspects of a digital identity, additional aspects of a real-world identity can be formed. Accordingly, as shown in FIG. 7, responsive to subscriber account identifier **405A** (1-303-555-1212) being concretely or authoritatively linked with subscriber **305A** (John Smith), an address of subscriber **305A** (John Smith) can also be authoritatively determined.

FIG. 8 is a diagram showing modifications to an identity network in an electronic or digital domain, according to an embodiment **800**. As indicated in FIG. 8, following a tie being made among aspects of an identity in an electronic or digital domain, a tie between a real-world identity and digital identity may utilize an aspect other than a subscriber account identifier. For example, as shown in FIG. 8, subscriber account identifier 1-303-555-1212 may no longer represent an exclusive conduit or tie between real-world subscriber **305A** (John Smith) and, for example, twitter handle **310B** (JS@hotdog_157) and/or email address **510** (jsmith957@gmail.com). Rather, as shown in FIG. 8, in view of electronic determinations of interactions between the real-world identity of subscriber **305A** (John Smith) and a particular mobile device (e.g., a device having a telephone

US 12,058,528 B2

23

number of 303-555-1212) additional ties in an identity network may stem from a particular communications device having a subscriber account identifier, for example. Accordingly, further revisions of the identity network of FIG. 8 may have no reliance on, and may thus exclude, the subscriber account number. In the example of FIG. 8, email addresses 510 and Twitter handle 310B of the real-life subscriber 305A (John Smith) may be authoritatively linked with a communications device located with subscriber 305A (John Smith) rather than with a subscriber account identifier of such communications device.

FIG. 9 is a diagram showing modifications to an identity network in an electronic or digital domain responsive to use of a one-time password, according to an embodiment 900. In FIG. 9, responsive to a social network (e.g., Facebook) transmitting a one-time password to a communications device co-located with real-world identity 820 (e.g., user: John Smith) a particular URL can be tied or bound directly to real-world identity 820 (John Smith). For example, communications device 905 (device XYZ) may be utilized to access a social network (Facebook) via a username and/or password corresponding to a subscriber. Social network 810 may be linked to subscriber identifier 405A, which corresponds to subscriber identifier 303-555-1212. However, responsive to one-time Facebook password 815 being conveyed to a communications device corresponding to subscriber account identifier 303-555-1212, the one-time password may provide the authoritative link between social network 810 (Facebook) and subscriber account identifier 405A. Additionally, responsive to subscriber account identifier 405A having a strong tie to social network 810, subscriber account identifier 405A may now be used to provide a tie to subscriber 305A (John Smith). Additionally, by way of a tie between subscriber account identifier 405A and subscriber 305A (John Smith), other digital identities can be determined, perhaps with increased authority.

FIG. 10 is a diagram showing a generalized identity network in an electronic or digital domain, according to an embodiment 1000. As shown in FIG. 10, responsive to establishing a plurality of ties between a real-world identity (e.g., via a subscriber account identifier, a persistent identifier, and/or a subscriber-unique alias) and an identity in an electronic or digital domain, logical groupings may be established in the electronic or digital domain. For example, as shown in FIG. 10, subscriber 305A (John Smith) represented in an electronic or digital domain may be represented by identities 1010 (digital identities) as well as devices 1005. Within a grouping of digital identities, social network 810 (Facebook) may be represented along with a user name associated with subscriber 305A having a particular username (User: John Smith). Likewise, in an electronic or digital domain, subscriber 305 (John Smith) may be represented via a grouping of devices 1005 comprising identifiers for ancillary devices owned or at least curated by subscriber 305A (John Smith) such as device 905 (device XYZ). Formation of such logical groupings (e.g., social network groupings, device groupings, and so forth) can bring about expansion of coverage of a digital identity and an electronic or digital domain.

FIG. 11, shows additional identity networks in an electronic or digital domain, according to an embodiment 1100. In the embodiment of FIG. 11, in response to electronic determination that various members of household 1105 ("Smith" household) may be residing at a similar or even identical IP address, such as may be the case in response to member 1115 (John Smith), member 1120 (Jenny Smith), and member 1125 (Patricia Smith) sharing or occupying the

24

same household and/or having a common (post office) mailing address. In particular embodiments, determining that John Smith, Jenny Smith, and Patricia Smith share or occupy the same household, may involve electronically determining an IP address of the router or other Wi-Fi device, for example, if such Wi-Fi devices are utilized to provide network conductivity to the members of the household. Additionally, as shown in FIG. 11, logical group 1130 (ancillary devices) may comprise devices operated by member 1115 (John Smith), such as device 1135 (a smart TV), device 1140 (a laptop computer), and device 1145 (an iPad), which, for example, may share John Smith's username and password. In this context, and "ancillary device" refers to an electronic device (e.g., smart TV 1135, laptop computer 1140, iPad 1145) that is owned or otherwise curated a subscriber, such as John Smith. An "ancillary device" may also refer to an IOT device, such as an automated garage door opener, sensor, or other device controlled and are curated by a subscriber.

FIG. 12 is an identity network showing interactions to modify ties in a subscriber's identity and electronic digital domain, according to an embodiment 1200. As shown in FIG. 12, members of household 1105 (the Smith household) having a physical address 1110 (123 Main Street). Members of household 1105 may all utilize, at least time to time, a landline/wireline telephone corresponding to a telephone number of 303-555-0123. In the embodiment of FIG. 12, even though the landline/wireline telephone may be registered in the name of John Smith, all members of the Smith household may be grouped as users of one or more ancillary devices (e.g., a landline/wireline telephone). Such ancillary devices, such as landline 1210, is physically located within the confines of the Smith household and under the care/duration of John, Jenny, and/or Patricia Smith. Accordingly, a direct tie may be made between household 1105 (the Smith household) and landline 1210 (corresponding to 303-555-0123). Further, landline 1210, along with mobile 1207, may form members of phones group 1205.

It may be appreciated that such expansions in customer relations management data may be achieved when querying any member of a particular household. Accordingly, identity networks can be expanded within households, increasing the overall knowledge possessed by a customer relations management system. Accordingly, by leveraging the digital-to-real-world connection, it becomes possible to create a domain-spanning network that ties digital identities and real-world identities.

In FIG. 13, computing device 702 may provide one or more sources of executable computer instructions in the form of physical states and/or signals (e.g., stored in memory states), for example. Computing device 1302 may communicate with computing device 1304 by way of a network connection, such as via network 1308, for example. As previously mentioned, a connection, while physical, may be virtual while not necessarily being tangible. Although computing device 1304 of FIG. 13 shows various tangible, physical components, claimed subject matter is not limited to a computing devices having only these tangible components as other implementations and/or embodiments may include alternative arrangements that may comprise additional tangible components or fewer tangible components, for example, that function differently while achieving similar results. Rather, examples are provided merely as illustrations. It is not intended that claimed subject matter be limited in scope to illustrative examples.

Memory 1322 may comprise any non-transitory storage medium. Memory 1322 may comprise, for example, primary

US 12,058,528 B2

25

memory 1324 and secondary memory 1326, additional memory circuits may be used. Memory 1322 may comprise, for example, random access memory, read only memory, etc., such as in the form of one or more storage devices and/or systems, such as, for example, a disk drive including an optical disc drive, a tape drive, a solid-state memory drive, etc., just to name a few examples.

Memory 1322 may comprise one or more articles utilized to store a program of executable computer instructions. For example, processor 1320 may fetch executable instructions from memory and proceed to execute the fetched instructions. Memory 1322 may also comprise a memory controller for accessing device readable-medium 1340 that may carry and/or make accessible digital content, which may include code, and/or instructions, for example, executable by processor 1320 and/or some other device, such as a controller, as one example, capable of executing computer instructions, for example. Under direction of processor 1320, a non-transitory memory, such as memory cells storing physical states (e.g., memory states), comprising, for example, a program of executable computer instructions, may be executed by processor 1320 and able to generate signals to be communicated via a network, for example, as previously described. Generated signals may also be stored in memory, also previously suggested.

Memory 1322 may store electronic files and/or electronic documents, such as relating to one or more users, and may also comprise a machine-readable medium that may carry and/or make accessible content, including code and/or instructions, for example, executable by processor 1320 and/or some other device, such as a controller, as one example, capable of executing computer instructions, for example. As previously mentioned, the term electronic file and/or the term electronic document are used throughout this document to refer to a set of stored memory states and/or a set of physical signals associated in a manner so as to thereby form an electronic file and/or an electronic document. That is, it is not meant to implicitly reference a particular syntax, format and/or approach used, for example, with respect to a set of associated memory states and/or a set of associated physical signals. It is further noted an association of memory states, for example, may be in a logical sense and not necessarily in a tangible, physical sense. Thus, although signal and/or state components of an electronic file and/or electronic document, are to be associated logically, storage thereof, for example, may reside in one or more different places in a tangible, physical memory, in an embodiment.

Algorithmic descriptions and/or symbolic representations are examples of techniques used by those of ordinary skill in the signal processing and/or related arts to convey the substance of their work to others skilled in the art. An algorithm is, in the context of the present patent application, and generally, is considered to be a self-consistent sequence of operations and/or similar signal processing leading to a desired result. In the context of the present patent application, operations and/or processing involve physical manipulation of physical quantities. Typically, although not necessarily, such quantities may take the form of electrical and/or magnetic signals and/or states capable of being stored, transferred, combined, compared, processed and/or otherwise manipulated, for example, as electronic signals and/or states making up components of various forms of digital content, such as signal measurements, text, images, video, audio, etc.

Processor 1320 may comprise one or more circuits, such as digital circuits, to perform at least a portion of a com-

26

puting procedure and/or process. By way of example, but not limitation, processor 1320 may comprise one or more processors, such as controllers, microprocessors, microcontrollers, application specific integrated circuits, digital signal processors, programmable logic devices, field programmable gate arrays, the like, or any combination thereof. In various implementations and/or embodiments, processor 1320 may perform signal processing, typically substantially in accordance with fetched executable computer instructions, such as to manipulate signals and/or states, to construct signals and/or states, etc., with signals and/or states generated in such a manner to be communicated and/or stored in memory, for example.

FIG. 13 also illustrates device 1304 as including a component 1332 operable with input/output devices, communication interface 1330, and communication bus 1315, for example, so that signals and/or states may be appropriately communicated between devices, such as device 1304 and an input device and/or device 1304 and an output device. A user may make use of an input device, such as a computer mouse, stylus, track ball, keyboard, and/or any other similar device capable of receiving user actions and/or motions as input signals. Likewise, for a device having speech to text capability, a user may speak to generate input signals. Likewise, a user may make use of an output device, such as a display, a printer, etc., and/or any other device capable of providing signals and/or generating stimuli for a user, such as visual stimuli, audio stimuli and/or other similar stimuli.

Example Implementation

A possible plan (among numerous possible plans) for implementation of a communications device information identity network may include the use of a database for providing graphs in an electronic or digital domain, which correspond to identity networks. However, in some instances, while such a database they be utilized to store an entirety of parameters corresponding to numerous real-world identities, relationships, and/or nodes corresponding to aspects of a real-world identity, it may be appreciated that modeling such identity networks can become computationally inefficient, especially in response to modeling certain types of relationships.

For example, in a graph database suitable for modeling identity networks, communications devices may be more tightly tied or attached to a real-world identity (e.g., user, subscriber, persona, etc.) via a device and SIM card. However, a SIM card may store parameters that relate or tie back to a communication services carrier. Accordingly, modeling real-world identities in an electronic or digital domain, such as corresponding to a ported device having a tie or other type of relationship with a new communication services carrier (such as by way of porting to a new communication services carrier) may point or be directed toward a new carrier.

In an example implementation, however, may give rise to an identity graph for a first communication services carrier may comprise, for example, over 100,000,000 edges. Such a large number of edges may result in such a node unduly inefficient sense, at least in some implementations, a graph databases suitable for modeling an identity network may operate most efficiently when no node includes more than a few dozen edges or relationships connected between or among nodes.

Additionally, it is possible that certain nodes of the graph to comprise or referring to sensitive content (e.g., personally identify information). In some instances, databases for providing graphs that correspond to identity networks may not

US 12,058,528 B2

27

be configured to operate in a manner that protects highly sensitive data, such as personally identifiable information, account numbers, etc. Further, applying parameters related to transactions in the graph database may introduce additional inefficiency. For example, a communications device that authenticates numerous times (e.g., between 10 and 30 times) may give rise to a threshold at which a graph corresponding to an identity network may approach, for example, tens of thousands of nodes (e.g., wherein each transaction may represent an aspect of electronic or digital identity) and edges (representing relationships between aspects of an electronic or digital entity) for a single subscriber. Accordingly, it may be appreciated that such a system could introduce process efficiencies especially as such relate to recovery of an identity in electronic or digital domain.

Thus, a hybrid system may be constructed, in which sensitive content is not stored within the graph (representing the identity network) directly. Rather, sensitive content or parameters may be stored in databases separate from databases utilized to store parameters related to subscriber identity networks. For example, transactional data may be best suited for storage within a transactional database, such as Hadoop, or Cassandra. Such databases are specifically designed around time-stamped, transactional data in large quantities, tied to a single key lookup (such as, in this instance, the persona or phone identifier, such as PID or PFA values.).

Hadoop refers to a distributed computing system, which employs a map-reduce type of architecture. In the context of the present patent application, the terms map-reduce architecture and/or similar terms are intended to refer to a distributed computing system implementation and/or embodiment for processing and/or for generating larger sets of signal samples employing map and/or reduce operations for a parallel, distributed process performed over a network of devices. A map operation and/or similar terms refer to processing of signals (e.g., signal samples) to generate one or more key-value pairs and to distribute the one or more pairs to one or more devices of the system (e.g., network). A reduce operation and/or similar terms refer to processing of signals (e.g., signal samples) via a summary operation (e.g., such as counting the number of real-world identities in a queue, yielding frequencies of subscriber account identifiers, persistent identifiers, etc.). A system may employ such an architecture, such as by marshaling distributed server devices, executing various tasks in parallel, and/or managing communications, such as signal transfers, between various parts of the system (e.g., network), in an embodiment. Hadoop refers to an open source implementation and/or embodiment of a map-reduce type architecture (available from the Apache Software Foundation, 1901 Munsey Drive, Forrest Hill, MD, 21050-2747), but may include other aspects, such as the Hadoop distributed file system (HDFS) (available from the Apache Software Foundation, 1901 Munsey Drive, Forrest Hill, MD, 21050-2747). In general, therefore, “Hadoop” and/or similar terms (e.g., “Hadoop-type,” etc.) refer to an implementation and/or embodiment of a scheduler for executing larger processing jobs using a map-reduce architecture over a distributed system. Furthermore, in the context of the present patent application, use of the term “Hadoop” is intended to include versions, presently known and/or to be later developed.

In addition, large quantities of textual data may be best stored in document databases, so the persona nodes in the electronic or digital domain need not contain a large history of data. In these instances, such data can instead be stored in

28

a document databases, again keyed or triggered by a smaller set of keys (e.g., PID, PFA, etc.) or an address identifier key, for example. Finally, large groupings of normalized data can be stored in relational databases. Thus, for example, in an instant such as described above, in which greater than 100,000,000 phone numbers may share a single communication services carrier, the data can be stored and related through a relational database, which does not suffer from slowdowns based, at least in part, on a large number of occurrences of related data.

Thus, by leveraging a hybrid system, utilizing databases specialized for particular types of data, it may be possible to optimize certain aspects of database management of identity networks so as to permit overall storage with increased speed.

A phone number, for example, or any other type of subscriber account identifier found through authentication, or a personal identifier such as a merchant’s customer ID, can be initially found in the graph database that represents an identity network. Finding such an identifier may be utilized to recover the persona or phone identifier corresponding to a real-world identity (e.g., subscriber, user, persona, etc.). In turn, such an identifier may be utilized as the key to the other databases, retrieving transactional data to enable building of a current picture of trust. Document data to build the underlying real-world identity and the identity in an electronic or digital domain corresponding to the real-world identity, and (as needed) relational data may be used to extract a picture of large and otherwise unwieldy connections.

Thus, such “separation of responsibility,” in which a plurality of databases may be permitted to perform optimally as a function of datatypes stored within each database, may permit optimal operation and management of a large-scale system of identity networks. Further, since each query can be performed in parallel with other queries, rapid association of all needed data corresponding to a real-world identity may provide a complete picture of a real-world identity, and time periods that do not exceed 50 milliseconds.

Accordingly, in an implementation, in response to a subscriber account identifier (e.g., a telephone number, persistent ID, and/or a subscriber-unique alias) being sent to an identity verifier in connection with any type of authentication, auditing, and/or verification operation, the phone number, being unique or at least virtually unique, may bring about a rapid lookup in the graph database, typically performed in under 10 ms. The subscriber account identifier edge nodes associated with the identifier, or aspects of a digital identity network, can be retrieved virtually instantly, and can be extended to retrieve the connected real-world identity as part of the initial search with little to no overhead. In general, it may be appreciated that in many instances accessing an identity graph in an electronic or digital domain may occur in non-real-time scenarios. Thus, even in response to a large number of entities, such as greater than 1000 (which may be relatively uncommon) accessing an identity graph in an electronic or digital domain need not represent any type of bottleneck in a subscriber authentication process.

In particular embodiments, responsive to a primary real-world entity node being retrieved from a node of an electronic or digital domain may be associated with keying parameters so as to permit retrieval of personally identifiable information, for example, from additional (secured) databases. For example, a retrieved key may permit retrieval of documents from a document database, and a PFA (Payfone Alias) or other subscriber-unique identifier may be utilized

US 12,058,528 B2

29

to identify and/or retrieve parameters relevant to databases that store transactions records. Thus, parameters relevant to various aspects of a subscriber's electronic or digital domain may be retrieved nearly instantaneously, and thus be ready for use on a real-time basis. In cases in which trustworthi-

ness parameters, trust scores, etc. are to be provided, separate transactional and document databases may be utilized to supply requested parameters.

In an instance in which a customer passes a customer ID (e.g., such as a transaction signed by a merchant), transactional parameters may be stored in a relational database, as each merchant could have thousands to millions of customer IDs. However, in a relational database, a customer ID may map directly to a real-world entity ID, which may represent a unique identifier of a node in a graph database representing the identity network in an electronic or digital domain. Accordingly, such maps may represent a series of brief accesses of unique identification parameters, which may characterize a number of aspects of a real-world subscriber. Accordingly, as described hereinabove, responsive to a real-world identifier (e.g., a subscriber account identifier, a persistent identifier, a subscriber-unique alias, etc.) has been obtained, relevant parameters data may be obtained in durations typically measured in single-digit milliseconds. Accordingly, it may be appreciated that parameters regarding a large number of subscribers may be obtained in a small fraction of a second.

In one instance, utilizing a simple, relatively rudimentary system, between 25,000 and 50,000 transactions per second are possible, while conducting database operations within normal parameters. Thus, the methodology outlined above is believed to be powerful yet highly performant.

In the context of the present patent application, the term "connection," the term "component" and/or similar terms are intended to be physical, but are not necessarily always tangible. Whether or not these terms refer to tangible subject matter, thus, may vary in a particular context of usage. As an example, a tangible connection and/or tangible connection path may be made, such as by a tangible, electrical connection, such as an electrically conductive path comprising metal or other conductor, that is able to conduct electrical current between two tangible components. Likewise, a tangible connection path may be at least partially affected and/or controlled, such that, as is typical, a tangible connection path may be open or closed, at times resulting from influence of one or more externally derived signals, such as external currents and/or voltages, such as for an electrical switch. Non-limiting illustrations of an electrical switch include a transistor, a diode, etc. However, a "connection" and/or "component," in a particular context of usage, likewise, although physical, can also be non-tangible, such as a connection between a client and a server over a network, particularly a wireless network, which generally refers to the ability for the client and server to transmit, receive, and/or exchange communications, as discussed in more detail later.

In a particular context of usage, such as a particular context in which tangible components are being discussed, therefore, the terms "coupled" and "connected" are used in a manner so that the terms are not synonymous. Similar terms may also be used in a manner in which a similar intention is exhibited. Thus, "connected" is used to indicate that two or more tangible components and/or the like, for example, are tangibly in direct physical contact. Thus, using the previous example, two tangible components that are electrically connected are physically connected via a tangible electrical connection, as previously discussed. However, "coupled," is used to mean that potentially two or more

30

tangible components are tangibly in direct physical contact. Nonetheless, "coupled" is also used to mean that two or more tangible components and/or the like are not necessarily tangibly in direct physical contact, but are able to cooperate, liaise, and/or interact, such as, for example, by being "optically coupled." Likewise, the term "coupled" is also understood to mean indirectly connected. It is further noted, in the context of the present patent application, since memory, such as a memory component and/or memory states, is intended to be non-transitory, the term physical, at least if used in relation to memory necessarily implies that such memory components and/or memory states, continuing with the example, are tangible.

Unless otherwise indicated, in the context of the present patent application, the term "or" if used to associate a list, such as A, B, or C, is intended to mean A, B, and C, here used in the inclusive sense, as well as A, B, or C, here used in the exclusive sense. With this understanding, "and" is used in the inclusive sense and intended to mean A, B, and C; whereas "and/or" can be used in an abundance of caution to make clear that all of the foregoing meanings are intended, although such usage is not required. In addition, the term "one or more" and/or similar terms is used to describe any feature, structure, characteristic, and/or the like in the singular, "and/or" is also used to describe a plurality and/or some other combination of features, structures, characteristics, and/or the like. Likewise, the term "based on" and/or similar terms are understood as not necessarily intending to convey an exhaustive list of factors, but to allow for existence of additional factors not necessarily expressly described.

Furthermore, it is intended, for a situation that relates to implementation of claimed subject matter and is subject to testing, measurement, and/or specification regarding degree, that the particular situation be understood in the following manner. As an example, in a given situation, assume a value of a physical property is to be measured. If alternatively reasonable approaches to testing, measurement, and/or specification regarding degree, at least with respect to the property, continuing with the example, is reasonably likely to occur to one of ordinary skill, at least for implementation purposes, claimed subject matter is intended to cover those alternatively reasonable approaches unless otherwise expressly indicated. As an example, if a plot of measurements over a region is produced and implementation of claimed subject matter refers to employing a measurement of slope over the region, but a variety of reasonable and alternative techniques to estimate the slope over that region exist, claimed subject matter is intended to cover those reasonable alternative techniques unless otherwise expressly indicated.

To the extent claimed subject matter is related to one or more particular measurements, such as with regard to physical manifestations capable of being measured physically, such as, without limit, temperature, pressure, voltage, current, electromagnetic radiation, etc., it is believed that claimed subject matter does not fall with the abstract idea judicial exception to statutory subject matter. Rather, it is asserted, that physical measurements are not mental steps and, likewise, are not abstract ideas.

It is noted, nonetheless, that a typical measurement model employed is that one or more measurements may respectively comprise a sum of at least two components. Thus, for a given measurement, for example, one component may comprise a deterministic component, which in an ideal sense, may comprise a physical value (e.g., sought via one or more measurements), often in the form of one or more

US 12,058,528 B2

31

signals, signal samples and/or states, and one component may comprise a random component, which may have a variety of sources that may be challenging to quantify. At times, for example, lack of measurement precision may affect a given measurement. Thus, for claimed subject matter, a statistical or stochastic model may be used in addition to a deterministic model as an approach to identification and/or prediction regarding one or more measurement values that may relate to claimed subject matter.

For example, a relatively large number of measurements may be collected to better estimate a deterministic component. Likewise, if measurements vary, which may typically occur, it may be that some portion of a variance may be explained as a deterministic component, while some portion of a variance may be explained as a random component. Typically, it is desirable to have stochastic variance associated with measurements be relatively small, if feasible. That is, typically, it may be preferable to be able to account for a reasonable portion of measurement variation in a deterministic manner, rather than a stochastic matter as an aid to identification and/or predictability.

Along these lines, a variety of techniques have come into use so that one or more measurements may be processed to better estimate an underlying deterministic component, as well as to estimate potentially random components. These techniques, of course, may vary with details surrounding a given situation. Typically, however, more complex problems may involve use of more complex techniques. In this regard, as alluded to above, one or more measurements of physical manifestations may be modelled deterministically and/or stochastically. Employing a model permits collected measurements to potentially be identified and/or processed, and/or potentially permits estimation and/or prediction of an underlying deterministic component, for example, with respect to later measurements to be taken. A given estimate may not be a perfect estimate; however, in general, it is expected that on average one or more estimates may better reflect an underlying deterministic component, for example, if random components that may be included in one or more obtained measurements, are considered. Practically speaking, of course, it is desirable to be able to generate, such as through estimation approaches, a physically meaningful model of processes affecting measurements to be taken.

In some situations, however, as indicated, potential influences may be complex. Therefore, seeking to understand appropriate factors to consider may be particularly challenging. In such situations, it is, therefore, not unusual to employ heuristics with respect to generating one or more estimates. Heuristics refers to use of experience related approaches that may reflect realized processes and/or realized results, such as with respect to use of historical measurements, for example. Heuristics, for example, may be employed in situations where more analytical approaches may be overly complex and/or nearly intractable. Thus, regarding claimed subject matter, an innovative feature may include, in an example embodiment, heuristics that may be employed, for example, to estimate and/or predict one or more measurements.

It is further noted that the terms “type” and/or “like,” if used, such as with a feature, structure, characteristic, and/or the like, using “optical” or “electrical” as simple examples, means at least partially of and/or relating to the feature, structure, characteristic, and/or the like in such a way that presence of minor variations, even variations that might otherwise not be considered fully consistent with the feature, structure, characteristic, and/or the like, do not in general prevent the feature, structure, characteristic, and/or the like

32

from being of a “type” and/or being “like,” (such as being an “optical-type” or being “optical-like,” for example) if the minor variations are sufficiently minor so that the feature, structure, characteristic, and/or the like would still be considered to be substantially present with such variations also present. Thus, continuing with this example, the terms optical-type and/or optical-like properties are necessarily intended to include optical properties. Likewise, the terms electrical-type and/or electrical-like properties, as another example, are necessarily intended to include electrical properties. It should be noted that the specification of the present patent application merely provides one or more illustrative examples and claimed subject matter is intended to not be limited to one or more illustrative examples; however, again, as has always been the case with respect to the specification of a patent application, particular context of description and/or usage provides helpful guidance regarding reasonable inferences to be drawn.

With advances in technology, it has become more typical to employ distributed computing and/or communication approaches in which portions of a process, such as signal processing of signal samples, for example, may be allocated among various devices, including one or more client devices and/or one or more server devices, via a computing and/or communications network, for example. A network may comprise two or more devices, such as network devices and/or computing devices, and/or may couple devices, such as network devices and/or computing devices, so that signal communications, such as in the form of signal packets and/or signal frames (e.g., comprising one or more signal samples), for example, may be exchanged, such as between a server device and/or a client device, as well as other types of devices, including between wired and/or wireless devices coupled via a wired and/or wireless network, for example.

In the context of the present patent application, the term network device refers to any device capable of communicating via and/or as part of a network and may comprise a computing device. While network devices may be capable of communicating signals (e.g., signal packets and/or frames), such as via a wired and/or wireless network, they may also be capable of performing operations associated with a computing device, such as arithmetic and/or logic operations, processing and/or storing operations (e.g., storing signal samples), such as in memory as tangible, physical memory states, and/or may, for example, operate as a server device and/or a client device in various embodiments. Network devices capable of operating as a server device, a client device and/or otherwise, may include, as examples, dedicated rack-mounted servers, desktop computers, laptop computers, set top boxes, tablets, netbooks, smart phones, wearable devices, integrated devices combining two or more features of the foregoing devices, and/or the like, or any combination thereof. As mentioned, signal packets and/or frames, for example, may be exchanged, such as between a server device and/or a client device, as well as other types of devices, including between wired and/or wireless devices coupled via a wired and/or wireless network, for example, or any combination thereof. It is noted that the terms, server, server device, server computing device, server computing platform and/or similar terms are used interchangeably. Similarly, the terms client, client device, client computing device, client computing platform and/or similar terms are also used interchangeably. While in some instances, for ease of description, these terms may be used in the singular, such as by referring to a “client device” or a “server device,” the description is intended to encompass one or more client devices and/or one or more server devices, as appropriate.

US 12,058,528 B2

33

Along similar lines, references to a “database” are understood to mean, one or more databases and/or portions thereof, as appropriate.

It should be understood that for ease of description, a network device (also referred to as a networking device) may be embodied and/or described in terms of a computing device and vice-versa. However, it should further be understood that this description should in no way be construed so that claimed subject matter is limited to one embodiment, such as a computing device exclusively and/or a network device exclusively, but, instead, may be embodied as a variety of devices or combinations thereof, including, for example, one or more illustrative examples.

A network may also include now known, and/or to be later developed arrangements, derivatives, and/or improvements, including, for example, past, present and/or future mass storage, such as network attached storage (NAS), a storage area network (SAN), and/or other forms of device readable media, for example. A network may include a portion of the Internet, one or more local area networks (LANs), one or more wide area networks (WANs), wire-line type connections, wireless type connections, other connections, or any combination thereof. Thus, a network may be worldwide in scope and/or extent. Likewise, sub-networks, such as may employ differing architectures and/or may be substantially compliant and/or substantially compatible with differing protocols, such as network computing and/or communications protocols (e.g., network protocols), may interoperate within a larger network.

In the context of the present patent application, the term sub-network and/or similar terms, if used, for example, with respect to a network, refers to the network and/or a part thereof. Sub-networks may also comprise links, such as physical links, connecting and/or coupling nodes, so as to be capable to communicate signal packets and/or frames between devices of particular nodes, including via wired links, wireless links, or combinations thereof. Various types of devices, such as network devices and/or computing devices, may be made available so that device interoperability is enabled and/or, in at least some instances, may be transparent. In the context of the present patent application, the term “transparent,” if used with respect to devices of a network, refers to devices communicating via the network in which the devices are able to communicate via one or more intermediate devices, such as one or more intermediate nodes, but without the communicating devices necessarily specifying the one or more intermediate nodes and/or the one or more intermediate devices of the one or more intermediate nodes and/or, thus, may include within the network the devices communicating via the one or more intermediate nodes and/or the one or more intermediate devices of the one or more intermediate nodes, but may engage in signal communications as if such intermediate nodes and/or intermediate devices are not necessarily involved. For example, a router may provide a link and/or connection between otherwise separate and/or independent LANs.

In the context of the present patent application, a “private network” refers to a particular, limited set of devices, such as network devices and/or computing devices, able to communicate with other devices, such as network devices and/or computing devices, in the particular, limited set, such as via signal packet and/or signal frame communications, for example, without a need for re-routing and/or redirecting signal communications. A private network may comprise a stand-alone network; however, a private network may also comprise a subset of a larger network, such as, for example,

34

without limitation, all or a portion of the Internet. Thus, for example, a private network “in the cloud” may refer to a private network that comprises a subset of the Internet. Although signal packet and/or frame communications (e.g. signal communications) may employ intermediate devices of intermediate nodes to exchange signal packets and/or signal frames, those intermediate devices may not necessarily be included in the private network by not being a source or designated destination for one or more signal packets and/or signal frames, for example. It is understood in the context of the present patent application that a private network may direct outgoing signal communications to devices not in the private network, but devices outside the private network may not necessarily be able to direct inbound signal communications to devices included in the private network.

The Internet refers to a decentralized global network of interoperable networks that comply with the Internet Protocol (IP). It is noted that there are several versions of the Internet Protocol. The term Internet Protocol, IP, and/or similar terms are intended to refer to any version, now known and/or to be later developed. The Internet includes local area networks (LANs), wide area networks (WANs), wireless networks, and/or long haul public networks that, for example, may allow signal packets and/or frames to be communicated between LANs. The term World Wide Web (WWW or Web) and/or similar terms may also be used, although it refers to a part of the Internet that complies with the Hypertext Transfer Protocol (HTTP). For example, network devices may engage in an HTTP session through an exchange of appropriately substantially compatible and/or substantially compliant signal packets and/or frames. It is noted that there are several versions of the Hypertext Transfer Protocol. The term Hypertext Transfer Protocol, HTTP, and/or similar terms are intended to refer to any version, now known and/or to be later developed. It is likewise noted that in various places in this document substitution of the term Internet with the term World Wide Web (“Web”) may be made without a significant departure in meaning and may, therefore, also be understood in that manner if the statement would remain correct with such a substitution.

Although claimed subject matter is not in particular limited in scope to the Internet and/or to the Web; nonetheless, the Internet and/or the Web may without limitation provide a useful example of an embodiment at least for purposes of illustration. As indicated, the Internet and/or the Web may comprise a worldwide system of interoperable networks, including interoperable devices within those networks. The Internet and/or Web has evolved to a public, self-sustaining facility accessible to potentially billions of people or more worldwide. Also, in an embodiment, and as mentioned above, the terms “WWW” and/or “Web” refer to a part of the Internet that complies with the Hypertext Transfer Protocol. The Internet and/or the Web, therefore, in the context of the present patent application, may comprise a service that organizes stored digital content, such as, for example, text, images, video, etc., through the use of hypermedia, for example. It is noted that a network, such as the Internet and/or Web, may be employed to store electronic files and/or electronic documents.

A Hyper Text Markup Language (“HTML”), for example, may be utilized to specify digital content and/or to specify a format thereof, such as in the form of an electronic file and/or an electronic document, such as a Web page, Web site, etc., for example. An Extensible Markup Language (“XML”) may also be utilized to specify digital content and/or to specify a format thereof, such as in the form of an

US 12,058,528 B2

35

electronic file and/or an electronic document, such as a Web page, Web site, etc., in an embodiment. Of course, HTML and/or XML are merely examples of “markup” languages, provided as non-limiting illustrations. Furthermore, HTML and/or XML are intended to refer to any version, now known and/or to be later developed, of these languages. Likewise, claimed subject matter are not intended to be limited to examples provided as illustrations, of course.

In the context of the present patent application, the term “Web site” and/or similar terms refer to Web pages that are associated electronically to form a particular collection thereof. Also, in the context of the present patent application, “Web page” and/or similar terms refer to an electronic file and/or an electronic document accessible via a network, including by specifying a URL for accessibility via the Web, in an example embodiment. As alluded to above, in one or more embodiments, a Web page may comprise digital content coded (e.g., via computer instructions) using one or more languages, such as, for example, markup languages, including HTML and/or XML, although claimed subject matter is not limited in scope in this respect. Also, in one or more embodiments, application developers may write code (e.g., computer instructions) in the form of JavaScript (or other programming languages), for example, executable by a computing device to provide digital content to populate an electronic document and/or an electronic file in an appropriate format, such as for use in a particular application, for example. Use of the term “JavaScript” and/or similar terms intended to refer to one or more particular programming languages are intended to refer to any version of the one or more programming languages identified, now known and/or to be later developed. Thus, JavaScript is merely an example programming language. As was mentioned, claimed subject matter is not intended to be limited to examples and/or illustrations.

In the context of the present patent application, the terms “entry,” “electronic entry,” “document,” “electronic document,” “content,” “digital content,” “item,” and/or similar terms are meant to refer to signals and/or states in a physical format, such as a digital signal and/or digital state format, e.g., that may be perceived by a user if displayed, played, tactilely generated, etc. and/or otherwise executed by a device, such as a digital device, including, for example, a computing device, but otherwise might not necessarily be readily perceivable by humans (e.g., if in a digital format). Likewise, in the context of the present patent application, digital content provided to a user in a form so that the user is able to readily perceive the underlying content itself (e.g., content presented in a form consumable by a human, such as hearing audio, feeling tactile sensations and/or seeing images, as examples) is referred to, with respect to the user, as “consuming” digital content, “consumption” of digital content, “consumable” digital content and/or similar terms. For one or more embodiments, an electronic document and/or an electronic file may comprise a Web page of code (e.g., computer instructions) in a markup language executed or to be executed by a computing and/or networking device, for example. In another embodiment, an electronic document and/or electronic file may comprise a portion and/or a region of a Web page. However, claimed subject matter is not intended to be limited in these respects.

Also, for one or more embodiments, an electronic document and/or electronic file may comprise a number of components. As previously indicated, in the context of the present patent application, a component is physical, but is not necessarily tangible. As an example, components with reference to an electronic document and/or electronic file, in

36

one or more embodiments, may comprise text, for example, in the form of physical signals and/or physical states (e.g., capable of being physically displayed). Typically, memory states, for example, comprise tangible components, whereas physical signals are not necessarily tangible, although signals may become (e.g., be made) tangible, such as if appearing on a tangible display, for example, as is not uncommon. Also, for one or more embodiments, components with reference to an electronic document and/or electronic file may comprise a graphical object, such as, for example, an image, such as a digital image, and/or sub-objects, including attributes thereof, which, again, comprise physical signals and/or physical states (e.g., capable of being tangibly displayed). In an embodiment, digital content may comprise, for example, text, images, audio, video, and/or other types of electronic documents and/or electronic files, including portions thereof, for example.

Also, in the context of the present patent application, the term parameters (e.g., one or more parameters) refer to material descriptive of a collection of signal samples, such as one or more electronic documents and/or electronic files, and exist in the form of physical signals and/or physical states, such as memory states. For example, one or more parameters, such as referring to an electronic document and/or an electronic file comprising an image, may include, as examples, time of day at which an image was captured, latitude and longitude of an image capture device, such as a camera, for example, etc. In another example, one or more parameters relevant to digital content, such as digital content comprising a technical article, as an example, may include one or more authors, for example. Claimed subject matter is intended to embrace meaningful, descriptive parameters in any format, so long as the one or more parameters comprise physical signals and/or states, which may include, as parameter examples, collection name (e.g., electronic file and/or electronic document identifier name), technique of creation, purpose of creation, time and date of creation, logical path if stored, coding formats (e.g., type of computer instructions, such as a markup language) and/or standards and/or specifications used so as to be protocol compliant (e.g., meaning substantially compliant and/or substantially compatible) for one or more uses, and so forth.

Signal packet communications and/or signal frame communications, also referred to as signal packet transmissions and/or signal frame transmissions (or merely “signal packets” or “signal frames”), may be communicated between nodes of a network, where a node may comprise one or more network devices and/or one or more computing devices, for example. As an illustrative example, but without limitation, a node may comprise one or more sites employing a local network address, such as in a local network address space. Likewise, a device, such as a network device and/or a computing device, may be associated with that node. It is also noted that in the context of this patent application, the term “transmission” is intended as another term for a type of signal communication that may occur in any one of a variety of situations. Thus, it is not intended to imply a particular directionality of communication and/or a particular initiating end of a communication path for the “transmission” communication. For example, the mere use of the term in and of itself is not intended, in the context of the present patent application, to have particular implications with respect to the one or more signals being communicated, such as, for example, whether the signals are being communicated “to” a particular device, whether the signals are being communicated “from” a particular device, and/or regarding which end of a communication path may be initiating

US 12,058,528 B2

37

communication, such as, for example, in a “push type” of signal transfer or in a “pull type” of signal transfer. In the context of the present patent application, push and/or pull type signal transfers are distinguished by which end of a communications path initiates signal transfer.

Thus, a signal packet and/or frame may, as an example, be communicated via a communication channel and/or a communication path, such as comprising a portion of the Internet and/or the Web, from a site via an access node coupled to the Internet or vice-versa. Likewise, a signal packet and/or frame may be forwarded via network nodes to a target site coupled to a local network, for example. A signal packet and/or frame communicated via the Internet and/or the Web, for example, may be routed via a path, such as either being “pushed” or “pulled,” comprising one or more gateways, servers, etc. that may, for example, route a signal packet and/or frame, such as, for example, substantially in accordance with a target and/or destination address and availability of a network path of network nodes to the target and/or destination address. Although the Internet and/or the Web comprise a network of interoperable networks, not all of those interoperable networks are necessarily available and/or accessible to the public.

In the context of the particular patent application, a network protocol, such as for communicating between devices of a network, may be characterized, at least in part, substantially in accordance with a layered description, such as the so-called Open Systems Interconnection (OSI) seven-layer type of approach and/or description. A network computing and/or communications protocol (also referred to as a network protocol) refers to a set of signaling conventions, such as for communication transmissions, for example, as may take place between and/or among devices in a network. In the context of the present patent application, the term “between” and/or similar terms are understood to include “among” if appropriate for the particular usage and vice-versa. Likewise, in the context of the present patent application, the terms “compatible with,” “comply with” and/or similar terms are understood to respectively include substantial compatibility and/or substantial compliance.

A network protocol, such as protocols characterized substantially in accordance with the aforementioned OSI description, has several layers. These layers are referred to as a network stack. Various types of communications (e.g., transmissions), such as network communications, may occur across various layers. The lowest level layer in a network stack, such as the so-called physical layer, may characterize how symbols (e.g., bits and/or bytes) are communicated as one or more signals (and/or signal samples) via a physical medium (e.g., twisted pair copper wire, coaxial cable, fiber optic cable, wireless air interface, combinations thereof, etc.). Progressing to higher-level layers in a network protocol stack, additional operations and/or features may be available via engaging in communications that are substantially compatible and/or substantially compliant with a particular network protocol at these higher-level layers. For example, higher-level layers of a network protocol may, for example, affect device permissions, user permissions, etc.

A network and/or sub-network, in an embodiment, may communicate via signal packets and/or signal frames, such via participating digital devices and may be substantially compliant and/or substantially compatible with, but is not limited to, now known and/or to be developed, versions of any of the following network protocol stacks: ARCNET, AppleTalk, ATM, Bluetooth, DECnet, Ethernet, FDDI, Frame Relay, HIPPI, IEEE 1394, IEEE 802.11, IEEE-488, Internet Protocol Suite, IPX, Myrinet, OSI Protocol Suite,

38

QsNet, RS-232, SPX, System Network Architecture, Token Ring, USB, and/or X.25. A network and/or sub-network may employ, for example, a version, now known and/or later to be developed, of the following: TCP/IP, UDP, DECnet, NetBEUI, IPX, AppleTalk and/or the like. Versions of the Internet Protocol (IP) may include IPv4, IPv6, and/or other later to be developed versions.

In one example embodiment, as shown in FIG. 13, a system embodiment may comprise a local network (e.g., device 1304 and medium 1340) and/or another type of network, such as a computing and/or communications network. For purposes of illustration, therefore, FIG. 13 shows an embodiment 1300 of a system that may be employed to implement either type or both types of networks. Network 1308 may comprise one or more network connections, links, processes, services, applications, and/or resources to facilitate and/or support communications, such as an exchange of communication signals, for example, between a computing device, such as 1302, and another computing device, such as 1306, which may, for example, comprise one or more client computing devices and/or one or more server computing device. By way of example, but not limitation, network 1308 may comprise wireless and/or wired communication links, telephone and/or telecommunications systems, Wi-Fi networks, Wi-MAX networks, the Internet, a local area network (LAN), a wide area network (WAN), or any combinations thereof.

Example devices in FIG. 13 may comprise features, for example, of a client computing device and/or a server computing device, in an embodiment. It is further noted that the term computing device, in general, whether employed as a client and/or as a server, or otherwise, refers at least to a processor and a memory connected by a communication bus. Likewise, in the context of the present patent application at least, this is understood to refer to sufficient structure within the meaning of 35 USC § 112 (f) so that it is specifically intended that 35 USC § 112 (f) not be implicated by use of the term “computing device” and/or similar terms; however, if it is determined, for some reason not immediately apparent, that the foregoing understanding cannot stand and that 35 USC § 112 (f), therefore, necessarily is implicated by the use of the term “computing device” and/or similar terms, then, it is intended, pursuant to that statutory section, that corresponding structure, material and/or acts for performing one or more functions be understood and be interpreted to be described at least in FIG. 13 and in the text associated with the foregoing figure of the present patent application.

FIG. 14 is a flowchart for a method forming an identity network representation of a communications device subscriber, according to an embodiment (1400). It should be noted that the disclosed embodiments, such as the embodiment of FIG. 14, are intended to embrace numerous variations, including methods that may include actions in addition to those depicted in the figures, actions performed in an order different than those depicted in the figures, as well as methods including fewer steps than those depicted. The method of FIG. 14 begins at 1405, which includes transmitting a message to a communications device, such as communications device 102, for example. The method may continue at 1410, which includes receiving a signal, in response to the transmitted message, to verify that a subscriber having a real-world identity is co-located with the communications device. 1415 may include establishing, in an electronic or digital domain, two or more nodes of an identity network corresponding to aspects of the real-world identity of the subscriber. The identity network may be

US 12,058,528 B2

39

attached or tied to the real-world identity via a persistent identifier, and the two or more nodes of the identity network may be linked via one or more relationships.

In the preceding description, various aspects of claimed subject matter have been described. For purposes of explanation, specifics, such as amounts, systems and/or configurations, as examples, were set forth. In other instances, well-known features were omitted and/or simplified so as not to obscure claimed subject matter. While certain features have been illustrated and/or described herein, many modifications, substitutions, changes and/or equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all modifications and/or changes as fall within claimed subject matter.

It has proven convenient at times, principally for reasons of common usage, to refer to such physical signals and/or physical states as bits, values, elements, parameters, symbols, characters, terms, numbers, numerals, measurements, content and/or the like. It should be understood, however, that all of these and/or similar terms are to be associated with appropriate physical quantities and are merely convenient labels. Unless specifically stated otherwise, as apparent from the preceding discussion, it is appreciated that throughout this specification discussions utilizing terms such as “processing,” “computing,” “calculating,” “determining,” “establishing,” “obtaining,” “identifying,” “selecting,” “generating,” and/or the like may refer to actions and/or processes of a specific apparatus, such as a special purpose computer and/or a similar special purpose computing and/or network device. In the context of this specification, therefore, a special purpose computer and/or a similar special purpose computing and/or network device is capable of processing, manipulating and/or transforming signals and/or states, typically in the form of physical electronic and/or magnetic quantities, within memories, registers, and/or other storage devices, processing devices, and/or display devices of the special purpose computer and/or similar special purpose computing and/or network device. In the context of this particular patent application, as mentioned, the term “specific apparatus” therefore includes a general purpose computing and/or network device, such as a general purpose computer, once it is programmed to perform particular functions, such as pursuant to program software instructions.

For one or more embodiments, a device, such as a computing device and/or networking device, may comprise, for example, any of a wide range of digital electronic devices, including, but not limited to, desktop and/or notebook computers, high-definition televisions, digital versatile disc (DVD) and/or other optical disc players and/or recorders, game consoles, satellite television receivers, cellular telephones, tablet devices, wearable devices, personal digital assistants, mobile audio and/or video playback and/or recording devices, Internet of Things (IOT) type devices, or any combination of the foregoing. Further, unless specifically stated otherwise, a process as described, such as with reference to flow diagrams and/or otherwise, may also be executed and/or affected, in whole or in part, by a computing device and/or a network device. A device, such as a computing device and/or network device, may vary in terms of capabilities and/or features. Claimed subject matter is intended to cover a wide range of potential variations. For example, a device may include a numeric keypad and/or other display of limited functionality, such as a monochrome liquid crystal display (LCD) for displaying text, for example. In contrast, however, as another example, a web-enabled device may include a physical and/or a virtual

40

keyboard, mass storage, one or more accelerometers, one or more gyroscopes, global positioning system (GPS) and/or other location-identifying type capability, and/or a display with a higher degree of functionality, such as a touch-sensitive color 2D or 3D display, for example.

A computing and/or network device may include and/or may execute a variety of now known and/or to be developed operating systems, derivatives and/or versions thereof, including computer operating systems, such as Windows, iOS, Linux, a mobile operating system, such as iOS, Android, Windows Mobile, and/or the like. A computing device and/or network device may include and/or may execute a variety of possible applications, such as a client software application enabling communication with other devices. For example, one or more messages (e.g., content) may be communicated, such as via one or more protocols, now known and/or later to be developed, suitable for communication of email, short message service (SMS), and/or multimedia message service (MMS), including via a network, such as a social network, formed at least in part by a portion of a computing and/or communications network, including, but not limited to, an Internet service provider, a social network platform, just to provide a few examples. A computing and/or network device may also include executable computer instructions to process and/or communicate digital content, such as, for example, textual content, digital multimedia content, and/or the like. A computing and/or network device may also include executable computer instructions to perform a variety of possible tasks, such as browsing, searching, playing various forms of digital content, including locally stored and/or streamed video, and/or games such as, but not limited to, fantasy sports leagues. The foregoing is provided merely to illustrate that claimed subject matter is intended to include a wide range of possible features and/or capabilities.

In some circumstances, operation of a memory device, such as a change in state from a binary one to a binary zero or vice-versa, for example, may comprise a transformation, such as a physical transformation. With particular types of memory devices, such a physical transformation may comprise a physical transformation of an article to a different state or thing. For example, but without limitation, for some types of memory devices, a change in state may involve an accumulation and/or storage of charge or a release of stored charge. Likewise, in other memory devices, a change of state may comprise a physical change, such as a transformation in magnetic orientation. Likewise, a physical change may comprise a transformation in molecular structure, such as from crystalline form to amorphous form or vice-versa. In still other memory devices, a change in physical state may involve quantum mechanical phenomena, such as, superposition, entanglement, and/or the like, which may involve quantum bits (qubits), for example. The foregoing is not intended to be an exhaustive list of all examples in which a change in state from a binary one to a binary zero or vice-versa in a memory device may comprise a transformation, such as a physical, but non-transitory, transformation. Rather, the foregoing is intended as illustrative examples.

What is claimed is:

1. A method comprising:

receiving, by an identity verifier computing device from a communications device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity; establishing, by the identity verifier computing device, a plurality of nodes of an identity network, wherein:

US 12,058,528 B2

41

the identity network exists in an electronic or digital domain,
 the identity network is associated with the real-world identity via a persistent identifier,
 each node in the plurality of nodes is associated with the persistent identifier via a set of links, and
 each link in the set of links includes a trustworthiness parameter;
 responsive to a first set of interactions by a first aspect of a set of aspects with at least a first node of the plurality of nodes, updating, by the identity verifier computing device, a first trustworthiness parameter of a first link between a second node of the plurality of nodes and a second aspect of the set of aspects; and
 transmitting, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device, wherein the verification is based, at least in part, on the first link.

2. The method of claim 1, wherein the persistent identifier comprises a subscriber-account identifier.

3. The method of claim 1, wherein the set of aspects comprises one or more of:
 an electronic mail address of the real-world identity,
 an Internet protocol address of the real-world identity,
 a wireline telephone number of the real-world identity,
 an identifier of an ancillary device,
 an institutional account of the real-world identity,
 a healthcare account, and/or
 a transaction account of the real-world identity.

4. The method of claim 3, further comprising:
 establishing one or more additional links between or among the plurality of nodes of the identity network responsive to one or more electronically determined events with respect to the real-world identity.

5. The method of claim 4, wherein the one or more electronically determined events with respect to the real-world identity correspond to one or more of a second set of interactions between the real-world identity and one or more aspects of the set of aspects.

6. The method of claim 5, further comprising:
 assigning a confidence score to the real-world identity in the electronic or digital domain; and
 revising the confidence score based, at least in part, on the one or more of the second set of interactions between the real-world identity and the one or more aspects of the set of aspects.

7. The method of claim 6, wherein the confidence score is based, at least in part, on one or more deterministic events with respect to the communications device.

8. The method of claim 6, further comprising accessing a data store to detect one or more deterministic events in relation to historical norms with respect to the communications device.

9. The method of claim 8, wherein the one or more deterministic events with respect to the communications device correspond to an online event, and wherein the online event comprises one or more of:

a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier,
 a purchase or replacement of the communications device,
 a removal and/or replacement of a subscriber identity module (SIM), and/or
 a password reset of the communications device.

42

10. The method of claim 1, further comprising:
 revising the plurality of nodes of the identity network to exclude the persistent identifier.

11. The method of claim 1, further comprising:
 grouping the plurality of nodes of the identity network into one or more relationship groups, wherein the one or more relationship groups comprise one or more of:
 a content group,
 a transactions group,
 a financial group,
 a family group,
 a household group,
 a group associated with a physical address of the subscriber,
 a social network group, and/or
 a merchant group.

12. An apparatus comprising:
 at least one processor of an identity verifier computing device coupled to at least one memory device of the identity verifier computing device to:

receive, by the identity verifier computing device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity;

establish, by the identity verifier computing device, a plurality of nodes of an identity network, wherein:
 the identity network exists in an electronic or digital domain;

the identity network is associated with the real-world identity via a persistent identifier,
 each node in the plurality of nodes is associated with the persistent identifier via a set of links, and
 each link in the set of links includes a trustworthiness parameter;

responsive to a first set of interactions by a first aspect of a set of aspects with at least a first node of the plurality of nodes, update, by the identity verifier computing device, a first trustworthiness parameter of a first link between a second node of the plurality of nodes and a second aspect of the set of aspects; and

transmit, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device, wherein the verification is based, at least in part, on the first link.

13. The apparatus of claim 12, wherein the persistent identifier comprises a subscriber account identifier.

14. The apparatus of claim 12, wherein the set of aspects comprises one or more of:

an electronic mail address of the real-world identity,
 an Internet protocol address of the real-world identity,
 a wireline telephone number of the real-world identity,
 an identifier of an ancillary device,
 an institutional account of the real-world identity,
 a healthcare account, and/or
 a transaction account of the real-world identity.

15. The apparatus of claim 14, wherein the at least one processor coupled of the identity verifier computing device to the at least one memory device of the identity verifier computing device are additionally to establish one or more additional links between or among the plurality of nodes of the identity network responsive to one or more electronically determined events with respect to the real-world identity, wherein the one or more electronically determined events with respect to the real-world identity correspond to one or more of a second set of interactions between the real-world identity and one or more aspects of the set of aspects.

US 12,058,528 B2

43

16. The apparatus of claim 15, wherein the at least one processor of the identity verifier computing device coupled to the at least one memory device of the identity verifier computing device are further to:

- assign a confidence score to the real-world identity in the electronic or digital domain based at least in part on one or more deterministic events with respect to the communications device; and
- revise the confidence score based, at least in part, on the one or more of the second set of interactions between the real-world identity and the one or more aspects of the set of aspects.

17. The apparatus of claim 16, wherein the at least one processor of the identity verifier computing device coupled to the at least one memory device of the identity verifier computing device are further to access a data store to detect one or more deterministic events in relation to historical norms with respect to the communications device.

18. The apparatus of claim 17, wherein the one or more deterministic events with respect to the communications device correspond to an online event, and wherein the online event comprises one or more of:

- a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier,
- a purchase or replacement of the communications device,
- a removal and/or replacement of a subscriber identity module (SIM), and/or
- a password reset of the communications device.

19. An article comprising:

- a non-transitory storage medium having instructions stored thereon which, when executed by a processor of an identity verifier computing device coupled to at least one memory of the identity verifier computing device, are operable to:

receive, by an identity verifier computing device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity;

establish, by the identity verifier computing device, a plurality of nodes of an identity network, wherein: the identity network exists in an electronic or digital domain;

the identity network is associated with the real-world identity via a persistent identifier,

each node in the plurality of nodes is associated with the persistent identifier via a set of links, and

each link in the set of links includes a trustworthiness parameter;

responsive to a first set of interactions by a first aspect of a set of aspects with at least a first node of the plurality of nodes, update, by the identity verifier computing device, a first trustworthiness parameter of a first link

44

between a second node of the plurality of nodes and a second aspect of the set of aspects; and
transmit, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device, wherein the verification is based, at least in part, on the first link.

20. The article of claim 19, wherein the stored instructions are additionally operable to revise the plurality of nodes of the identity network to exclude the persistent identifier.

21. The article of claim 19, wherein the set of aspects comprises one or more of:

- an electronic mail address of the real-world identity,
- an Internet protocol address of the real-world identity,
- a wireline telephone number of the real-world identity,
- an identifier of an ancillary device,
- an institutional account of the real-world identity,
- a healthcare account, and/or
- a transaction account of the real-world identity.

22. The article of claim 21, wherein the stored instructions are additionally operable to establish one or more additional links between or among the plurality of nodes of the identity network responsive to one or more electronically determined events with respect to the real-world identity, wherein the one or more electronically determined events with respect to the real-world identity correspond to one or more of a second set of interactions between the real-world identity and one or more aspects of the set of aspects.

23. The article of claim 22, wherein stored instructions are additionally operable to:

- assign a confidence score to the real-world identity in the electronic or digital domain based at least in part on one or more deterministic events with respect to the communications device; and
- revise the confidence score based, at least in part, on the one or more of the second set of interactions between the real-world identity and the one or more aspects of the set of aspects.

24. The article of claim 23, wherein the stored instructions are additionally operable to access a data store to detect one or more deterministic events in relation to historical norms with respect to the communications device.

25. The article of claim 24, wherein the one or more deterministic events with respect to the communications device correspond to an online event, and wherein the online event comprises one or more of:

- a reassignment of a subscriber account identifier from a first communication services carrier to a second communication services carrier,
- a purchase or replacement of the communications device,
- a removal and/or replacement of a subscriber identity module (SIM), and/or
- a password reset of the communications device.

* * * * *

EXHIBIT B

US012200816B2

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

(10) **Patent No.:** **US 12,200,816 B2**
(45) **Date of Patent:** **Jan. 14, 2025**

(54) **TRANSMITTING A COMPLEMENT OF USER PARAMETERS TO A COMMUNICATIONS DEVICE**

(58) **Field of Classification Search**
CPC H04W 12/72; H04W 8/20
See application file for complete search history.

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

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,049,712 A 4/2000 Wallinder
8,145,561 B1 3/2012 Zhu
(Continued)

FOREIGN PATENT DOCUMENTS

EP 1197928 4/2002
KR 20060077541 7/2006
(Continued)

OTHER PUBLICATIONS

Anonymous, Method and Apparatus for Mobile Identity Authentication, Publication Date Mar. 29, 2010, 71 pages.

(Continued)

Primary Examiner — Shantell L Heiber

(74) *Attorney, Agent, or Firm* — Husch Blackwell LLP;
Bryan D. Stewart; Matthew C. Francis

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

(21) Appl. No.: **18/188,847**

(22) Filed: **Mar. 23, 2023**

(65) **Prior Publication Data**

US 2023/0232208 A1 Jul. 20, 2023

Related U.S. Application Data

(63) Continuation of application No. 17/570,335, filed on Jan. 6, 2022.

(Continued)

(51) **Int. Cl.**

H04W 4/00 (2018.01)

H04W 8/20 (2009.01)

(Continued)

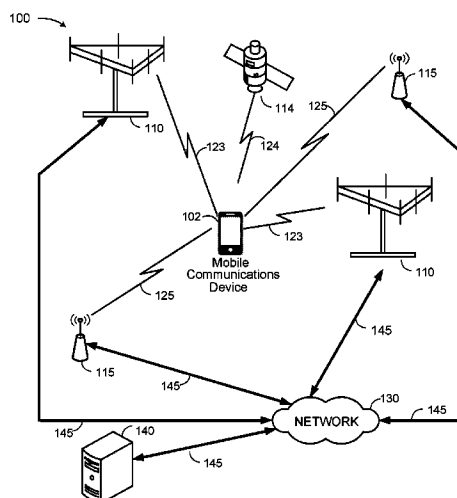
(52) **U.S. Cl.**

CPC **H04W 8/20** (2013.01); **H04W 12/71** (2021.01); **H04W 12/72** (2021.01); **H04W 12/75** (2021.01)

(57) **ABSTRACT**

Briefly, example methods, apparatuses, and/or articles of manufacture may be implemented, in whole or in part, using one or more computing devices to obtain, from a communications device, an identifier of the communications device transmitted via a communications network. The communications network may transmit a request for one or more parameters unique to a subscriber of the communications network. The method may also include processing signals indicative of the requested one or more parameters in response to the subscriber entering the one or more parameters into a graphical user interface of the communications device. The method may further include transmitting, to the communications device, one or more signals to provide a complement of subscriber parameters.

20 Claims, 5 Drawing Sheets



US 12,200,816 B2

Page 2

Related U.S. Application Data				2015/0215305	A1 *	7/2015	Wetzel		H04W 12/06	726/9			
(60)	Provisional application No. 63/134,914, filed on Jan. 7, 2021.			2015/0242601	A1	8/2015	Griffiths						
				2015/0332031	A1	11/2015	Mistry						
				2016/0012465	A1	1/2016	Sharp						
				2016/0050203	A1	2/2016	Hefetz						
(51)	Int. Cl.			2016/0057623	A1	2/2016	Dutt						
				2016/0103996	A1	4/2016	Salajegheh						
				2016/0110528	A1	4/2016	Gupta						
				2016/0180068	A1	6/2016	Das						
	H04W 12/71		(2021.01)	2016/0182503	A1	6/2016	Cheng						
				2016/0278664	A1	6/2016	Pant						
				2016/0197918	A1	7/2016	Turgeman						
				2016/0295512	A1	9/2016	Hara						
	H04W 12/72		(2021.01)	2016/0330199	A1	10/2016	Weiner						
				2016/0342784	A1	11/2016	Beveridge						
				2016/0350591	A1	12/2016	Kraft						
				2017/0063852	A1	3/2017	Azar						
	H04W 12/75		(2021.01)	2017/0085564	A1	3/2017	Giobbi						
				2017/0085565	A1	3/2017	Sheller						
				2017/0199588	A1	7/2017	Ahn						
				2017/0289168	A1	10/2017	Bar						
(56)	References Cited			2017/0337364	A1	11/2017	Whaley						
				2018/0078179	A1	3/2018	Deng						
				2018/0121921	A1	5/2018	Woo						
				2018/0181741	A1	6/2018	Whaley						
	U.S. PATENT DOCUMENTS			2019/0245851	A1	8/2019	Whaley						
				2019/0251534	A1	8/2019	Desai						
				2019/0281442	A1	9/2019	Kim						
				2019/0295006	A1	9/2019	Zises						
				2019/0325445	A1 *	10/2019	Anderson		G07G 1/0036				
				2019/0349767	A1	11/2019	Rolfe						
				2019/0370777	A1	12/2019	Brody						
				2020/0068381	A1 *	2/2020	Akhtar		H04L 65/1045				
				2020/0092723	A1	3/2020	McClement						
				2020/0104829	A1	4/2020	Arora et al.						
				2020/0134151	A1	4/2020	Magi						
				2020/0162515	A1	5/2020	Dubinsky						
				2020/0252218	A1	8/2020	Wexler						
				2020/0258084	A1	8/2020	Henderson						
				2020/0260258	A1	8/2020	Desai						
				2020/0304985	A1 *	9/2020	Gupta		H04W 4/70				
				2020/0342086	A1	10/2020	Oung						
				2020/0351818	A1 *	11/2020	Park		H04W 4/90				
				2022/0004611	A1	1/2022	Whaley						
				2022/0045852	A1	2/2022	Isshiki						
				2022/0075856	A1	3/2022	Whaley						
				2022/0374864	A1 *	11/2022	Agarwal		H04W 12/65				
				FOREIGN PATENT DOCUMENTS									
KR				20070121618	12/2007								
KR				20080003760	1/2008								
				OTHER PUBLICATIONS									
“Get Real-Time Feedback From Your Customers, without the Need for an Internet Connection” USSD Notifications HTTPS://txtnation.com/mobile-messaging/USSD-notifications/ , accessed Jun. 9, 2021 5 pages.													
Carr, “Mobile Payment Systems and Services: An Introduction”, Mobile Payment Forum, 2007, 12 pages.													
Karnouskos et al., “Mobile Payments: A journey through Existing Procedures and Standardization Initiatives,” IEEE communications Surveys and Tutorials, Fourth Quarter, vol. 6, Nov. 2004, 23 pages.													
Petrova, “Mobile Payment: Towards a Customer-Centric Model”, Web Information Systems Engineering—WISE Workshops, Sep. 2008, 13 pages.													
Rahimian, et al., “MPaySmart: A Customer Centric Approach in Offering Efficient Mobile Payments,” IEEE Asia-Pacific Services Computing Conference, Dec. 2008, 6 pages.													
Matsunaka et al., “Device Authentication and Registration Method Assisted by a Cellular System for User-driven Service Creation Architecture”; https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4784731 >, 2009 6th IEEE Consumer Communications and Networking Conference; Jan. 10-13, 2009, 5 pages.													

US 12,200,816 B2

Page 3

(56)

References Cited**OTHER PUBLICATIONS**

Soghoian, et al "Merx: Secure and Privacy Preserving Delegated Payments," Second International Trusted Computing Conference, Apr. 2009, 23 pages.

U.S. Appl. No. 14/518,765, filed Oct. 20, 2014, 86 pages.

U.S. Appl. No. 14/518,765 Filing Receipt mailed Oct. 27, 2014, 4 pages.

U.S. Appl. No. 14/518,765 Notice of Publication mailed Apr. 21, 2016, 1 page.

U.S. Appl. No. 14/518,765 Non-Final Office Action mailed May 17, 2017, 49 pages.

U.S. Appl. No. 14/518,765 Response to Non-Final Office Action filed Jun. 9, 2017, 27 pages.

U.S. Appl. No. 14/518,765 Notice of Allowance mailed Oct. 11, 2017, 25 pages.

U.S. Appl. No. 14/518,765 Issue Fee Payment and 312 Amendment filed Jan. 10, 2018, 27 pages.

U.S. Appl. No. 14/518,765 Amendment After Allowance Initialed by Examiner mailed Jan. 16, 2018, 1 page.

U.S. Appl. No. 14/518,765 Issue Notification mailed Feb. 7, 2018, 1 page.

U.S. Appl. No. 15/867,630, filed Jan. 10, 2018, 101 pages.

U.S. Appl. No. 15/867,630, Notice to File Missing Parts mailed Feb. 1, 2018, 3 pages.

U.S. Appl. No. 15/867,630, Filing Receipt mailed Feb. 1, 2018, 3 pages.

U.S. Appl. No. 15/867,630, Response to Missing Parts and Preliminary Amendment, filed Mar. 30, 2018, 22 pages.

U.S. Appl. No. 15/867,630, Updated Filing Receipt mailed Apr. 3, 2018, 4 pages.

U.S. Appl. No. 15/867,630, Notice of Publication mailed Jul. 12, 2018, 1 page.

U.S. Appl. No. 15/867,630, Non-Final Office Action mailed Oct. 11, 2018, 95 pages.

U.S. Appl. No. 15/867,630, Response to Non-Final Office Action filed Feb. 11, 2019, 27 pages.

U.S. Appl. No. 15/867,630, Final Office Action mailed Apr. 18, 2019, 28 pages.

U.S. Appl. No. 15/867,630, Response to Final Office Action and AFCP Request filed Jul. 18, 2019, 28 pages.

U.S. Appl. No. 15/867,630, Terminal Disclaimer filed and accepted Aug. 6, 2019, 7 pages.

U.S. Appl. No. 15/867,630, Notice of Allowance/Allowability mailed Aug. 20, 2019, 26 pages.

U.S. Appl. No. 15/867,630, Supplemental Notice of Allowability and Examiner Interview Summary mailed Nov. 6, 2019, 9 pages.

U.S. Appl. No. 15/867,630, Issue Fee Payment and 312 Response dated Nov. 11, 2019, 8 pages.

U.S. Appl. No. 15/867,630, Supplemental Notice of Allowability and Examiner Interview Summary mailed Nov. 29, 2019, 10 pages.

U.S. Appl. No. 15/867,630, Issue Notification dated Dec. 18, 2019, 1 page.

U.S. Appl. No. 16/691,490, filed Nov. 21, 2019, 98 pages.

U.S. Appl. No. 16/691,490 Filing Receipt mailed Dec. 10, 2019, 5 pages.

U.S. Appl. No. 16/691,490 Non-final Office Action dated Aug. 6, 2020, 54 pages.

U.S. Appl. No. 16/691,490 Response to Non-final Office Action and Terminal Disclaimer dated Aug. 6, 2020, 23 pages.

U.S. Appl. No. 16/691,490 Final Office Action dated Jan. 14, 2021, 37 pages.

U.S. Appl. No. 16/691,490 Amendment and AFCP Request filed Mar. 15, 2021, 18 pages.

U.S. Appl. No. 16/691,490 Advisory Action mailed Mar. 22, 2021, 4 pages.

U.S. Appl. No. 16/691,490 Request for Continued Examination and Amendment filed Apr. 14, 2021, 21 pages.

U.S. Appl. No. 16/691,490 Office Action mailed May 24, 2021, 67 pages.

U.S. Appl. No. 16/691,490 Amendment filed Aug. 24, 2021, 17 pages.

U.S. Appl. No. 16/691,490 Notice of Allowance/Allowability dated Nov. 26, 2021, 18 pages.

U.S. Appl. No. 16/691,490 Request for Updated Filing Receipt filed Feb. 3, 2022, 18 pages.

U.S. Appl. No. 16/691,490 Updated Filing Receipt dated Feb. 8, 2022, 4 pages.

U.S. Appl. No. 16/691,490 Request for Corrected Filing Receipt dated Feb. 10, 2022, 26 pages.

U.S. Appl. No. 16/691,490 Corrected Filing Receipt Dated Feb. 14, 2022, 4 pages.

U.S. Appl. No. 16/691,490 Issue Fee Payment and 312 Response filed Jan. 23, 2022, 6 pages.

U.S. Appl. No. 16/691,490 Issue Notification dated Mar. 16, 2022, 1 page.

U.S. Appl. No. 17/674,627, filed Feb. 17, 2022, 88 pages.

U.S. Appl. No. 17/674,627 Filing Receipt and Notice to File Missing Parts dated Feb. 25, 2022, 6 pages.

U.S. Appl. No. 17/674,627 Preliminary Amendment and Response to Notice to File Missing Parts filed Apr. 14, 2022, 13 pages.

U.S. Appl. No. 17/674,627 Updated Filing Receipt dated Apr. 18, 2022, 4 pages.

U.S. Appl. No. 17/674,627 Non-Final Office Action dated Nov. 10, 2022, 21 pages.

U.S. Appl. No. 17/674,627 Response to Non-Final Office action dated Feb. 10, 2023, 12 pages.

U.S. Appl. No. 17/570,335, filed Jan. 6, 2022, 65 pages.

U.S. Appl. No. 17/570,335 Filing Receipt dated Jan. 20, 2022, 4 pages.

U.S. Appl. No. 17/570,335 Notice of Publication dated Jul. 7, 2022, 1 page.

PCT Application PCT/US22/11725 PCT Application filed Jan. 7, 2022, 61 pages.

PCT Application PCT/US22/11725 International Search Report and Written Opinion dated Mar. 30, 2022, 15 pages.

PCT Application PCT/US2022/011725 Demand & Response to Written Opinion filed Oct. 31, 2022, 14 pages.

U.S. Appl. No. 17/225,964, filed Apr. 8, 2021, 81 pages.

U.S. Appl. No. 17/225,964 Filing Receipt dated Apr. 16, 2021, 3 pages.

U.S. Appl. No. 17/225,964 Non-final Office Action dated May 2, 2022, 32 pages.

U.S. Appl. No. 17/225,964 Examiner Interview Summary dated May 27, 2022, 3 pages.

U.S. Appl. No. 17/225,964 Response to Non-Final Office Action filed Jun. 6, 2022, 11 pages.

U.S. Appl. No. 17/225,964 Non-final Office Action dated Aug. 24, 2022, 19 pages.

U.S. Appl. No. 17/225,964 Response to Non-Final Office Action filed Nov. 23, 2022, 15 pages.

U.S. Appl. No. 17/225,964 Final Office Action dated Mar. 3, 2023, 33 pages.

PCT Application PCT/US22/23938 PCT Application filed Apr. 7, 2022, 71 pages.

PCT Application PCT/US22/23938 International Search Report and Written Opinion dated May 17, 2022, 11 pages.

U.S. Appl. No. 17/747,214, filed May 18, 2022, 63 pages.

U.S. Appl. No. 17/747,214 Filing Receipt dated May 24, 2022, 3 pages.

PCT Application PCT/US2022/29852 PCT Application filed May 18, 2022, 61 pages.

PCT Application PCT/US2022/029852 International Search Report and Written Opinion dated Oct. 6, 2022, 12 pages.

U.S. Appl. No. 17/410,918, filed Aug. 24, 2021, 79 pages.

U.S. Appl. No. 17/410,918 Filing Receipt dated Sep. 3, 2021, 4 pages.

U.S. Appl. No. 17/410,918 Notice of Publication dated Mar. 2, 2023, 1 page.

U.S. Appl. No. 15/600,140, filed May 19, 2017, 49 pages.

U.S. Appl. No. 15/600,140 Filing Receipt dated Jun. 5, 2017, 3 pages.

US 12,200,816 B2

Page 4

(56)

References Cited**OTHER PUBLICATIONS**

U.S. Appl. No. 15/600,140 Notice of Publication dated Nov. 23, 2017, 1 page.
 U.S. Appl. No. 15/600,140 Restriction Requirement dated May 24, 2019, 6 pages.
 U.S. Appl. No. 15/600,140 Response to Restriction Requirement dated May 28, 2019, 11 pages.
 U.S. Appl. No. 15/600,140 Non-final Office Action dated Sep. 11, 2019, 11 pages.
 U.S. Appl. No. 15/600,140 Terminal Disclaimer and Response to Non-final Office Action dated Dec. 11, 2019, 19 pages.
 U.S. Appl. No. 15/600,140 Final Office Action dated Jan. 7, 2020, 19 pages.
 U.S. Appl. No. 15/600,140 Terminal Disclaimer, Request for Continued Examination and Amendment filed Apr. 7, 2020, 24 pages.
 U.S. Appl. No. 15/600,140 Non-final Office Action dated Jun. 10, 2020, 21 pages.
 U.S. Appl. No. 15/600,140 Response to Non-final Office Action dated Sep. 2, 2020, 15 pages.
 U.S. Appl. No. 15/600,140 Final Office Action dated Dec. 2, 2020, 23 pages.
 U.S. Appl. No. 15/600,140 Response to Final Office Action dated Dec. 28, 2020, 12 pages.
 U.S. Appl. No. 15/600,140 Advisory Action dated Jan. 8, 2021, 6 pages.
 U.S. Appl. No. 15/600,140 Request for Continued Examination and Amendment filed Jan. 15, 2021, 22 pages.
 U.S. Appl. No. 15/600,140 Non-final Office Action dated Feb. 21, 2021, 22 pages.
 U.S. Appl. No. 15/600,140 Response to Non-final Office Action filed Apr. 16, 2021, 16 pages.
 U.S. Appl. No. 15/600,140 Notice of Allowance / Allowability dated Jul. 8, 2021, 16 pages.
 U.S. Appl. No. 15/600,140 Issue Fee Payment and Request for Corrected Filing Receipt filed Oct. 8, 2021, 28 pages.
 U.S. Appl. No. 15/600,140 Corrected Filing Receipt filed Oct. 12, 2021, 4 pages.
 U.S. Appl. No. 15/600,140 Corrected Notice of Allowability dated Oct. 20, 2021, 5 pages.
 U.S. Appl. No. 15/600,140 Issue Notification dated Oct. 27, 2021, 1 page.
 U.S. Appl. No. 17/527,083, filed Nov. 15, 2021, 62 pages.
 U.S. Appl. No. 17/527,083 Filing Receipt dated Nov. 30, 2021, pages.
 U.S. Appl. No. 17/527,083 Notice of Publication dated Mar. 10, 2022, 1 page.
 U.S. Appl. No. 17/475,191, filed Sep. 14, 2021, 61 pages.
 U.S. Appl. No. 17/475,191 Filing Receipt dated Sep. 27, 2021, 4 pages.
 U.S. Appl. No. 17/475,191 Notice of Publication dated Jan. 6, 2022, 1 page.
 U.S. Appl. No. 15/905,607, filed Feb. 26, 2018, 58 pages.
 U.S. Appl. No. 15/905,607 Filing Receipt mailed Mar. 23, 2018, 4 pages.
 U.S. Appl. No. 15/905,607 Notice of Publication mailed Jun. 28, 2018, 1 page.

U.S. Appl. No. 15/905,607 Issue Fee Payment filed Nov. 6, 2018, 6 pages.
 U.S. Appl. No. 15/905,607 Office Action mailed Nov. 14, 2019, 35 pages.
 U.S. Appl. No. 15/905,607 Terminal Disclaimer and Amendment filed Feb. 14, 2020, 25 pages.
 U.S. Appl. No. 15/905,607 Final Office Action mailed May 14, 2020, 30 pages.
 U.S. Appl. No. 15/905,607 Request for Continued Examination and Amendment filed Aug. 13, 2020, 26 pages.
 U.S. Appl. No. 15/905,607 Notice of Allowance/Allowability mailed Sep. 25, 2020, 22 pages.
 U.S. Appl. No. 15/905,607 Issue Fee Payment filed Nov. 6, 2020, 6 pages.
 U.S. Appl. No. 15/905,607 Issue Notification mailed Nov. 24, 2020, 1 Page.
 U.S. Appl. No. 16/385,776, filed Apr. 16, 2019, 46 pages.
 U.S. Appl. No. 16/385,776 Filing Receipt mailed Apr. 30, 2019, 5 pages.
 U.S. Appl. No. 16/385,776 Notice of Publication mailed Aug. 8, 2019, 1 page.
 U.S. Appl. No. 16/385,776 Office Action mailed Nov. 19, 2020, 42 Pages.
 U.S. Appl. No. 16/385,776 Amendment filed Dec. 28, 2020, 22 pages.
 U.S. Appl. No. 16/385,776 Final Office Action mailed Mar. 29, 2021, 38 pages.
 U.S. Appl. No. 16/385,776 Request for Continued Examination and Amendment filed Jun. 4, 2021, 26 pages.
 U.S. Appl. No. 16/385,776 Office Action mailed Sep. 15, 2021, 34 pages.
 U.S. Appl. No. 16/385,776 Response to Office Action filed Dec. 15, 2021, 23 pages.
 U.S. Appl. No. 16/385,776 Examiner Interview Summary dated Jan. 5, 2022, 2 pages.
 U.S. Appl. No. 16/385,776 Terminal Disclaimer and Request for Corrected Filing Receipt filed Jan. 6, 2022, 26 pages.
 U.S. Appl. No. 16/385,776 Notice of Allowance/Allowability dated Feb. 2, 2022, 9 pages.
 U.S. Appl. No. 16/385,776 Issue Fee Payment and 312 Amendment filed Apr. 28, 2022, 20 pages.
 U.S. Appl. No. 16/385,776 Examiner Response to 312 Amendment dated May 4, 2022, 3 pages.
 U.S. Appl. No. 16/385,776 Issue Notification dated Jun. 1, 2022, 1 page.
 U.S. Appl. No. 17/674,627 Terminal Disclaimer filed May 26, 2023, 5 pages.
 U.S. Appl. No. 17/674,627 Notice of Allowance and Allowability dated Jun. 8, 2023, 20 pages.
 U.S. Appl. No. 17/225,964 Response to Final Office Action & AFCP Request filed May 3, 2023, 23 pages.
 U.S. Appl. No. 17/225,964 Advisory Action issued Jun. 2, 2023, 10 pages.
 U.S. Appl. No. 17/225,964 RCE & Amendment filed Jul. 3, 2023, pp. 27.
 U.S. Appl. No. 17/410,918 Non-Final Office Action issued Jun. 1, 2023, 52 pages.

* cited by examiner

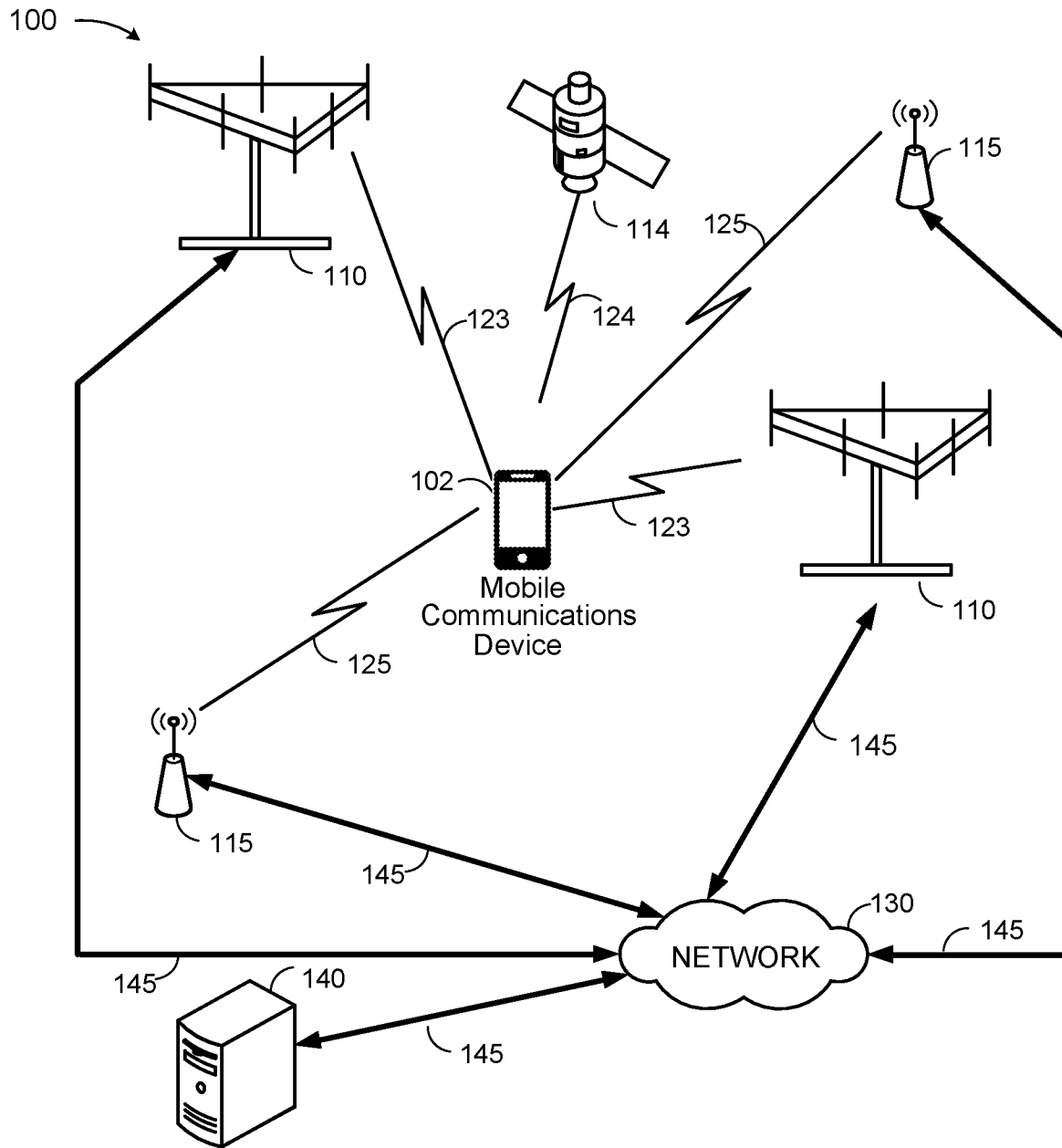


FIG. 1

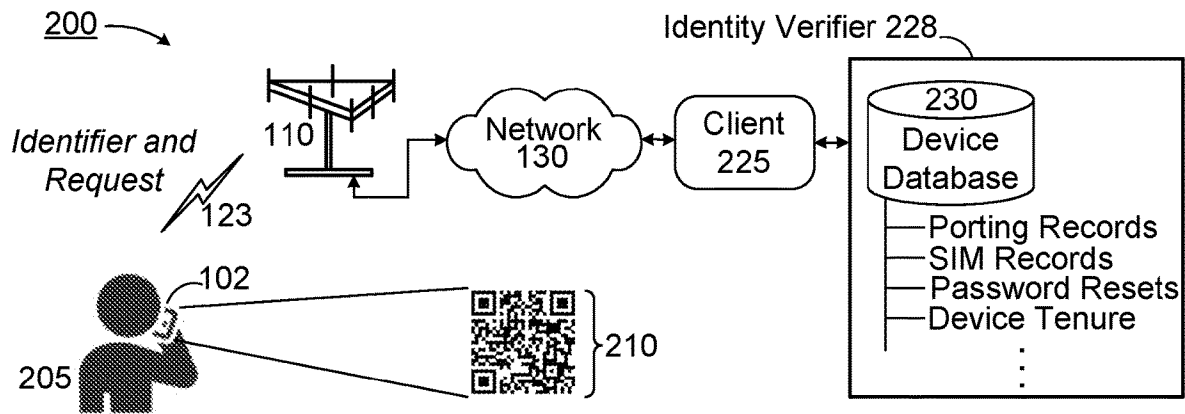


FIG. 2

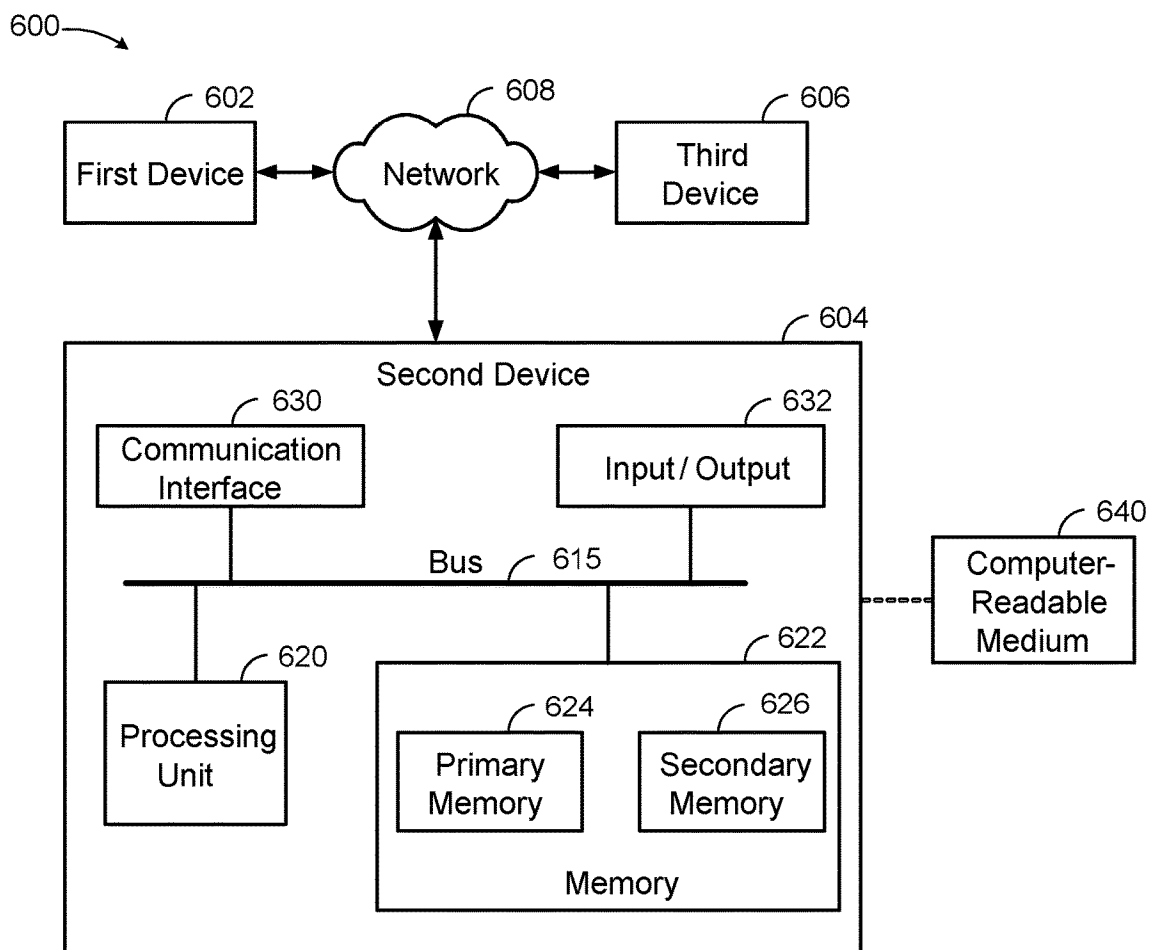
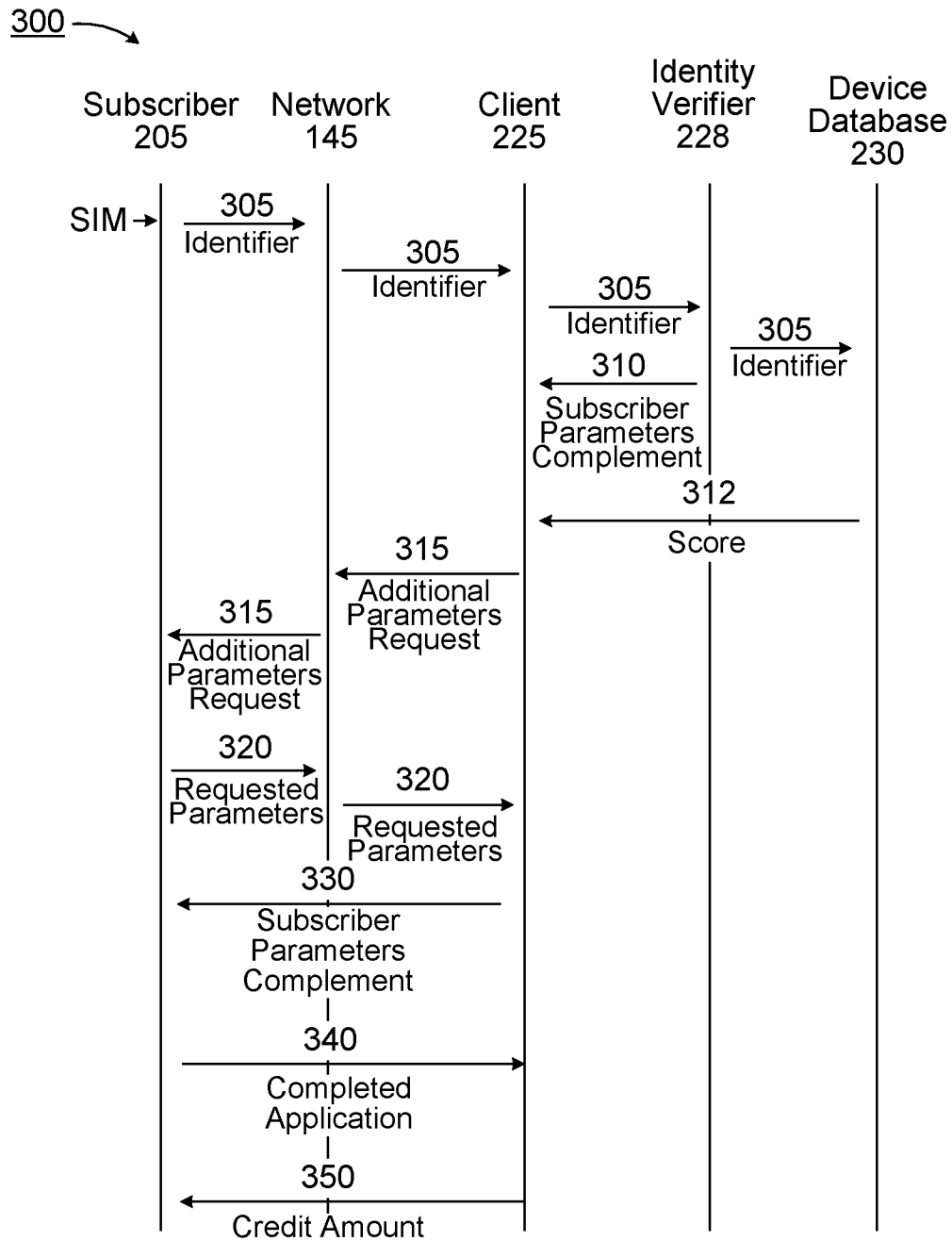


FIG. 6

U.S. Patent**Jan. 14, 2025****Sheet 3 of 5****US 12,200,816 B2****FIG. 3**

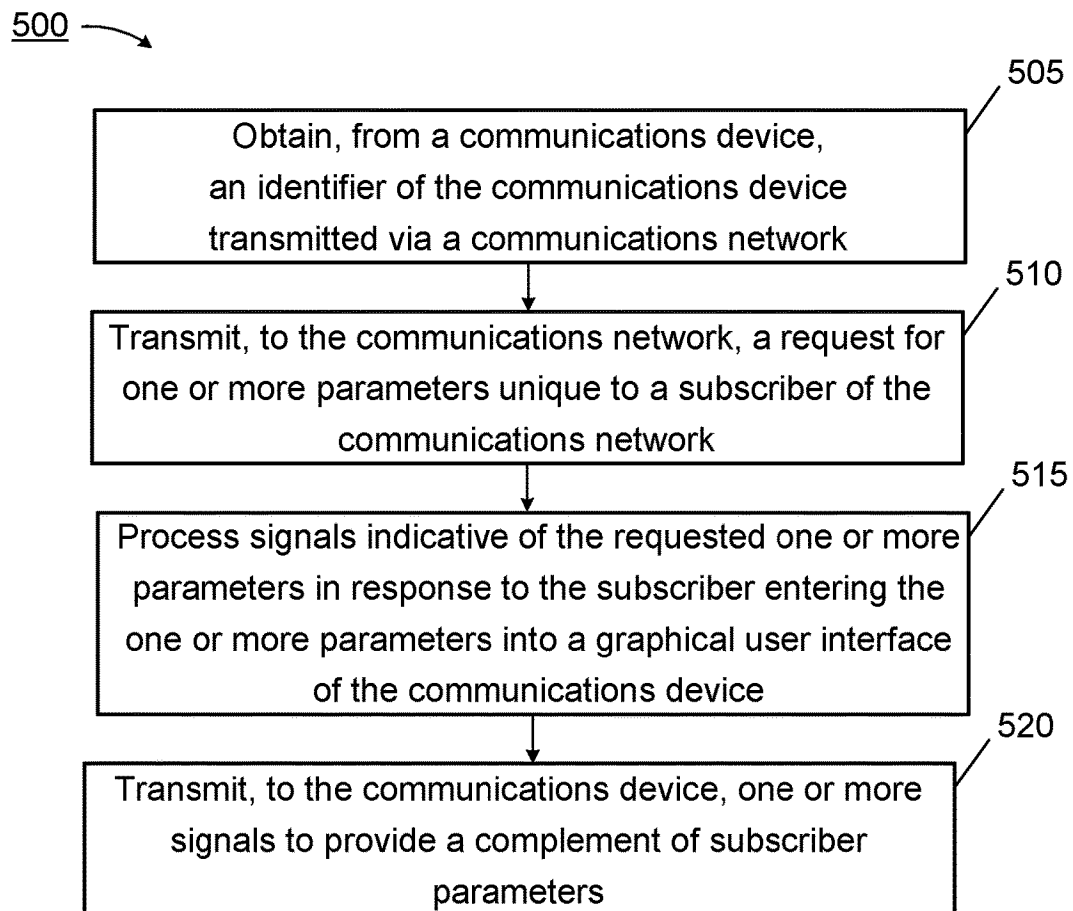
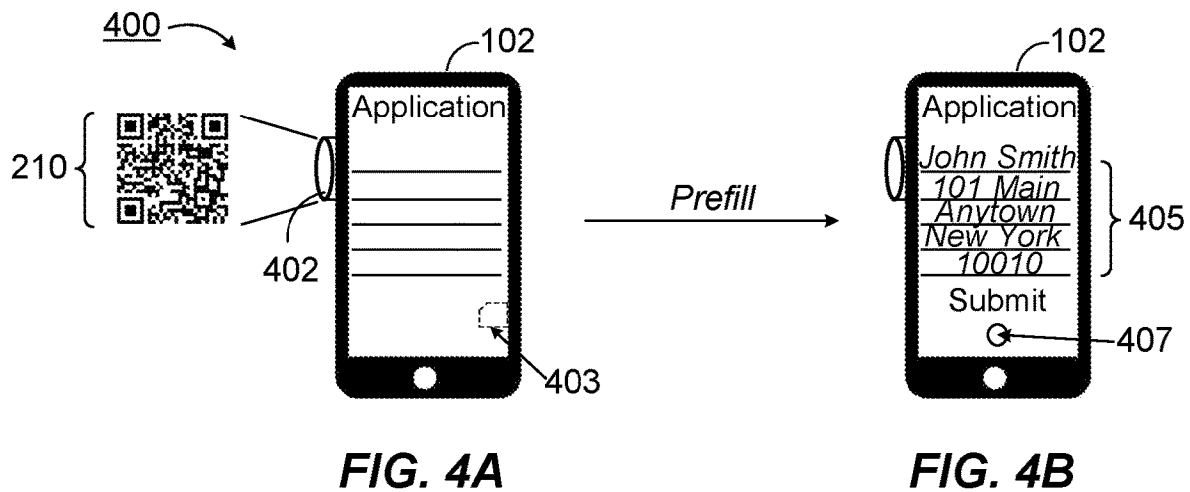


FIG. 5

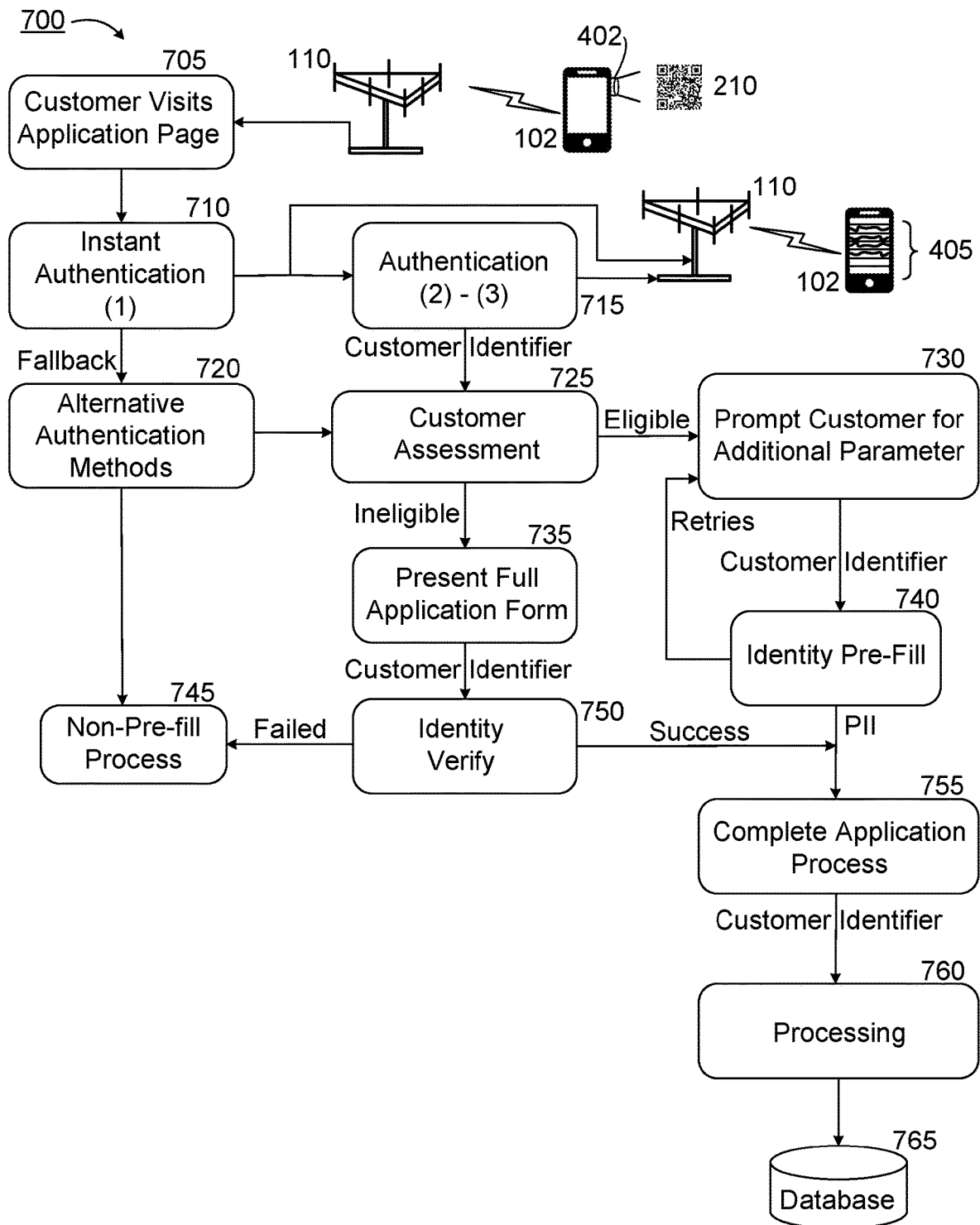


FIG. 7

US 12,200,816 B2

1

TRANSMITTING A COMPLEMENT OF USER PARAMETERS TO A COMMUNICATIONS DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. application Ser. No. 17/570,335, filed

Jan. 6, 2022, which claims the benefit of the priority date of U.S. provisional patent application No. 63/134,914, filed Jan. 7, 2021. The content of these applications is incorporated herein by reference in its entirety and for all purposes.

BACKGROUND

1. Field

The present disclosure relates generally to approaches for receiving signals, at a communications device, which relate to parameters of a subscriber co-located with the communications device, in which at least certain parameters are to be displayed on a user interface of the device.

2. Information

The World Wide Web or simply the Web, as provided by the Internet, has grown rapidly in recent years at least partially in response to the relative ease by which a wide variety of types of transactions can be performed or enabled via the Internet. As a consequence of widely available Internet connections, including connections to the Internet facilitated by mobile cellular communication services, a mobile subscriber may shop and/or browse for virtually any product and/or service utilizing a mobile communications device. Further, it may be appreciated that such an ability to shop and/or browse via a mobile communications device may involve only a portion or aspect of an overall mobile device-facilitated shopping ecosphere. Other aspects of a device-facilitated shopping ecosphere involve an ability to apply for and to obtain credit that can be used for the purchase of goods and services, and so forth.

However, it may also be appreciated that certain types of mobile communications devices, such as handheld mobile cellular telephones, tablet computing devices, and other mobile communications devices that operate without suitably-sized keyboard, for example, may present data-entry challenges to users. For example, a subscriber attempting to complete an application for credit utilizing a handheld mobile communications device (e.g., a smart phone, tablet computing device, etc.) may find it time-consuming and frustrating to enter a name, current address, past address(es), present employer, past employer(s), credit history, etc., utilizing a small touchscreen. Further, such data entry, utilizing small-form keyboards/keypads, may easily introduce errors which may, in turn, bring about the need for a subscriber to re-enter personal data so that the credit application, for example, can be completed. Thus, attempts to increase the ease and efficiency by which users can enter parameters into smaller-sized keyboards/keypads of, for example, handheld mobile communications devices, continues to be an active area of investigation.

SUMMARY

One general aspect concerns a method, which includes obtaining, from a communications device, an identifier of

2

the communications device transmitted via a communications network. The method also includes transmitting, to the communications network, a request for one or more parameters unique to a subscriber of the communications network.

5 The method also includes processing signals indicative of the requested one or more parameters in response to the subscriber entering the one or more parameters into a graphical user interface of the communications device. The method also includes transmitting, to the communications device, one or more signals to provide a complement of subscriber parameters.

10 Particular embodiments of the method may further include receiving a captured image of one or more machine-readable layouts, via the communications device, prior to transmitting the identifier. In particular embodiments, the one or more machine-readable layouts are arranged as a quick response (QR) code. In particular embodiments, the identifier of the communications device may be obtained in response to accessing a subscriber identity module (SIM) of a communications device. In particular embodiments, the identifier of the communications device may include an international mobile subscriber identifier (IMSI), an international mobile electronic identifier (IMEI), or a mobile station international subscriber directory number (MSISDN), or any combination thereof. In particular 15 embodiments, the communications network forms a part of a mobile cellular communications network. In particular embodiments, the one or more parameters unique to the subscriber includes at least one of a portion of a social security number and a date-of-birth. Particular embodiments may include transmitting to the communications device, one or more numerical values to the subscriber. In particular embodiments, the one or more numerical values may correspond to a credit value requested by the subscriber. In particular embodiments, the one or more numerical values may include a credit limit and/or an incentive amount. In particular embodiments, the complement of subscriber parameters includes, at least, a physical address of the subscriber.

20 Another general aspect refers to an apparatus that includes a processor coupled to a memory to initiate reception of an authentication request, transmitted by a subscriber co-located with a communications device, to populate a graphical user interface of the communications device with a complement of parameters indicative of the subscriber. The apparatus is also to initiate access of a data store to determine, responsive to receipt of the authentication request, in which the complement of parameters is indicative of the subscriber co-located with the communications device. The apparatus is also to initiate transmission of the complement of parameters indicative of the subscriber to the communications device.

25 In particular embodiments, the processor coupled to the memory is additionally to initiate determination of a measure of trust corresponding to the communications device in response to one or more accesses of the data store. In particular embodiments, the processor coupled to the memory is additionally to initiate processing of signals that represent a captured image of one or more machine-readable layouts transmitted by the communications device. In particular embodiments, the transmission initiated by the processor includes one or more signals indicative of a physical address of the subscriber. In particular embodiments the authentication request includes parameters indicative of an image of a quick response (QR) code captured by an imaging device accessible to the communications device. In particular embodiments, the authentication request includes 30

US 12,200,816 B2

3

an international mobile subscriber identifier (IMSI), an international mobile electronic identifier (IMEI), or a mobile subscriber international subscriber identification number (MSISDN), or any combination thereof.

Another general aspect refers to an article including a non-transitory storage medium having instructions stored thereon executable by a special-purpose computing platform to receive signals indicative of an identifier of a communications device from a communications network. The executable instructions may be additionally to bring about transmission, to the communications network, of a request for one or more parameters unique to a subscriber of the communications network. The executable instructions are additionally to bring about reception, from the communications network, of signals indicative of the requested one or more parameters. The executable instructions may be additionally to bring about transmission, to a mobile communications device, of one or more signals indicative of a complement of parameters indicative of the subscriber.

In particular embodiments, the complement of parameters of the subscriber includes parameters indicative of a physical address of the subscriber. The non-transitory storage medium includes instructions to determine a measure of trustworthiness of the communications device. In particular embodiments, the complement of parameters indicative of the subscriber may be accompanied by one or more numerical values transmitted to the subscriber. In particular embodiments, the one or more numerical values transmitted to the subscriber may include a credit value requested by the subscriber and/or an incentive amount. In particular embodiments, the communications network forms part of a mobile cellular communications network.

BRIEF DESCRIPTION OF THE DRAWINGS

Claimed subject matter is particularly pointed out and distinctly claimed in the concluding portion of the specification. However, both as to organization and/or method of operation, features, and/or advantages thereof, it may best be understood by reference to the following detailed description if read with the accompanying drawings in which:

FIG. 1 is a diagram of a communications device situated within a cellular communications infrastructure, according to various embodiments.

FIG. 2 shows a subscriber interacting with an aspect of a cellular communications network, within a cellular communications infrastructure, to obtain a complement of subscriber parameters, according to an embodiment.

FIG. 3 shows a message flow diagram in a method of transmitting a complement of subscriber parameters to a communications device, according to an embodiment.

FIG. 4A shows a communications device displaying an interface to accept a complement of subscriber parameters, according to an embodiment.

FIG. 4B shows a communications device displaying a user interface into which a complement of subscriber parameters has been pre-filled into the user interface, according to an embodiment.

FIG. 5 shows a process of transmitting a complement of subscriber parameters to a communications device, according to an embodiment.

FIG. 6 is a diagram showing a computing environment, according to an embodiment.

FIG. 7 shows a flowchart for a process of transmitting a complement of subscriber parameters to a communications device, according to an embodiment.

4

Reference is made in the following detailed description to the accompanying drawings, which form a part hereof, wherein like numerals may designate like parts throughout that are corresponding and/or analogous. It will be appreciated that the figures have not necessarily been drawn to scale, such as for simplicity and/or clarity of illustration. For example, dimensions of some aspects may be exaggerated relative to others, one or more aspects, properties, etc. may be omitted, such as for ease of discussion, or the like. Further, it is to be understood that other embodiments may be utilized. Furthermore, structural and/or other changes may be made without departing from claimed subject matter. References throughout this specification to "claimed subject matter" refer to subject matter intended to be covered by one or more claims, or any portion thereof, and are not necessarily intended to refer to a complete claim set, to a particular combination of claim sets (e.g., method claims, apparatus claims, etc.), or to a particular claim.

DETAILED DESCRIPTION

References throughout this specification to one implementation, an implementation, one embodiment, an embodiment, and/or the like means that a particular feature, structure, characteristic, and/or the like described in relation to a particular implementation and/or embodiment is included in at least one implementation and/or embodiment of claimed subject matter. Thus, appearances of such phrases, for example, in various places throughout this specification, are not necessarily intended to refer to the same implementation and/or embodiment or to any one particular implementation and/or embodiment. Furthermore, it is to be understood that particular features, structures, characteristics, and/or the like described, are capable of being combined in various ways in one or more implementations and/or embodiments and, therefore, are within intended claim scope. In general, of course, for the specification of a patent application, these and other issues have a potential to vary in a particular context of usage. In other words, throughout the disclosure, particular context of description and/or usage provides guidance regarding reasonable inferences to be drawn; however, likewise, the term "in this context" in general without further qualification refers at least to the context of the present patent application.

As previously alluded to, in an environment in which electronic communication devices, mobile cellular telephones, voice over Internet protocol (VoIP) communications devices, etc., have become ubiquitous, a communications device subscriber may wish to perform an electronic or digital transaction. Such electronic or digital transactions may comprise completing an application for credit, engaging in an electronic financial transaction, purchasing a product or service, applying for a loan, completing one or more forms of an application for healthcare or while visiting a health provider's office, and completing many other types of electronic documents. To facilitate such transactions, a subscriber co-located with a personal electronic communications device may establish an identity, such as may be established in connection with an electronic communications device subscriber account, such as with a cellular or mobile communications device services carrier, a VoIP services provider, or with any other type of communication services carrier. Establishment of an device subscriber account for use with a communications device, utilizing, for example, a subscriber account identifier, may permit the identity of an subscriber attempting to engage in an electronic or digital transaction to be authenticated, authorized,

US 12,200,816 B2

5

and/or verified. In some instances, given the nature of electronic or digital transactions, such as in an environment in which electronic or digital transactions may be initiated via a communications device at any time and at any location, it may be useful to be able to verify and/or authenticating the subscriber relatively quickly, such as in a real-time or near-real-time manner.

As a general matter, verification of a transacting party, such as via use of a communications device, may be desirable in response to an institution or organization (e.g., third party, etc.) seeking to determine the identity of a transacting party (e.g., a mobile subscriber). Verification of a transacting party may involve establishing a correspondence and/or association of the transacting party with a persistent subscriber account identifier, as demonstrated below through illustrative examples. In this context, a correspondence, association, and/or similar terms refer to a persistent, continuing and objectively verifiable relationship between a transacting party in possession of, for example, a particular communications device (such as a mobile communications device). Thus, a unique subscriber account identifier may be employed to signify and/or identify a particular transacting party. In this context, the term “mobile communications device identity” and/or similar terms refer to an identity that relies on a mobile communications device account relationship (also referred to as a correspondence and/or association) of a subscriber as a source of authenticating, authorizing, and/or verifying a transacting party and is capable of being verified by another (e.g., a third-party auditing, authorizing and/or verifying entity). The term “mobile subscriber device account” and/or similar terms in this context refer to a mobile communication services provider account. The terms “mobile communications device services provider,” “mobile communications device carrier,” “mobile network operator” may be used interchangeably. Furthermore, in this context, the term “mobile device services carrier,” “telecommunication services carrier,” “service carrier,” or simply “carrier” may refer to an entity of a communications infrastructure that provides wired and/or wireless communication services to the general public for a consideration, such as a monthly subscription fee.

Thus, a carrier (e.g., a telecommunication services carrier) may comprise a mobile communication services provider and/or mobile network operator. However, there are examples of carriers that may not correspond to mobile communications device services providers and/or mobile network operators. Such instances may include wireline services providers (for example, providers of services operating within the public switched telephone network or PSTN), which include wireline services for rotary dial telephones and/or telephones utilizing, for example, dual tone multi-frequency (DTMF) signaling. Accordingly, the terms “services carrier” or simply “carrier” may be used in place of a communication services carrier, such as a provider of mobile communication services and/or wireline telephone services provider without a loss in meaning and/or understanding. In a given situation, particular context of usage indicate if a term is being used in its most general sense or in a narrow sense, such as referring to a mobile communications device services provider, wireline services provider, mobile paging services provider, or mobile network operator, for example.

It is noted that while a correspondence or association between a transacting party and a communications device need not be long-term, such correspondence or association between a transacting party and a communications device should imply some amount of persistence to be of use in this

6

context. Other aspects of verifying and/or authenticating a mobile subscriber are described in greater detail later. For example, in an embodiment, verifying and/or authenticating a transacting party may relate to an account (e.g., a mobile account) and a subscriber (e.g., a mobile subscriber). Further, a subscriber account is one example of a type of subscriber account, especially in a networked electronic commerce environment, although claimed subject matter is not intended to be limited to online accounts or to mobile accounts. Rather, the term “account” or “subscriber account” in this context refers to a formal business arrangement between an entity, person, or other type of transacting party, and a provider of the account in order to accomplish a business purpose, for example. The term “account” is intended to be broadly interpreted as an arrangement that provides certain privileges. In this context, such privileges may involve access to credit, so as to permit the purchase of goods or services, access to privileged content, such as premium entertainment content (e.g., premium sports, cinema, or other entertainment content). Also in this context, the term “privileged content” is intended to be interpreted broadly and to encompass any type of content available exclusively to certain individuals and/or certain entities in response to supplying certain credentials. Also in this context the term “parameter” refers to a numerical or other measurable factor capable of defining a system and/or sets conditions for operation of a system. Thus, for example, a set of parameters may include data or information stored via a non-transitory memory that form or define, at least in part, an electronic representation of the state of a subscriber.

Likewise, an account may comprise attributes associated with or corresponding to the account. In this context, the term “subscriber account identifier” refers to a unique descriptor or feature associated with the account that defines certain aspects of the account. For example, as nonlimiting illustrations, with respect to a mobile device subscriber, a subscriber account identifier may include a mobile telephone number, a mobile subscriber-unique alias, an international mobile subscriber identifier (IMSI), Integrated Circuit Card Identifier (ICC ID), a mobile services and/or other type of identifier (e.g., a unique identifier) employed in connection with the particular mobile network operator or the mobile communication services provider. Mobile communications networks may include those compatible or compliant with a Global System for Mobile Communications (GSM) communications network, for example. Other examples of mobile subscriber account identifiers may include an International Mobile Equipment Identifier (IMEI), Mobile Station International Subscriber Directory Number (MSISDN), a mobile equipment identifier or any other identifier a mobile billing account number/identifier.

As discussed herein, a subscriber co-located with a communications device may apply for an account, such as a credit account, for example, or any other type of account that imparts or confers particular privileges to the subscriber. In many instances, to obtain such privileges, a communications device subscriber may be required to complete an application, such as an application for an account, an application for credit, and application for an increase in credit, or any other type of formal request involving the subscriber supplying subscriber-specific information, data, parameters, and so forth. However, as previously alluded to, completing an application for such privileges (e.g., a line of credit) may involve the subscriber interacting with a user interface of a communications device having a small-form keyboard, keypad, etc. Such data entry, utilizing small-form keyboards/keypads, may easily introduce errors which may, in turn,

US 12,200,816 B2

7

bring about the need for a subscriber to re-enter personal data so that the credit application, for example, can be completed.

Thus, in particular embodiments, a complement of subscriber-specific parameters may be conveyed to a communications device, so as to facilitate the relatively effortless completion of various user interface activities. For example, as may be involved in the completion of a credit application, a subscriber may be requested to enter a complement of parameters into an online application via a communications device. In certain embodiments, a subscriber faced with the task of entering a complement of subscriber-specific parameters (e.g., name, address, Social Security number, date-of-birth, past/present addresses, past/present employers, etc.) may need only engage in a few simple operations, via a communications device, so that a user interface (e.g., a graphical user interface) of the communications device may be populated or pre-filled with a complement of subscriber-specific parameters. In particular embodiments, an authenticator may access a centralized repository subscriber parameters so that a complement of subscriber parameters may be transmitted to the communications device. In particular embodiments, transmission of a complement of subscriber parameters, or significant portion thereof, may be automatically (e.g., without subscriber input) transmitted to a subscriber's communications device. A communications device may operate to automatically (e.g., without subscriber input) pre-fill, for example, a credit application. Transmission of a complement of subscriber parameters to a mobile communications device may involve conveying subscriber-specific parameters accessed from the centralized repository to the subscriber's mobile communications device.

In particular instances, transmission of a complement of subscriber parameters to a communications device from a centralized repository may occur responsive to capturing an image of a machine-readable layout (e.g., a quick response or "QR" code). Responsive to capturing such an image, one or more processors of a communications device (e.g., a mobile communications device) may access a memory area of the communications device (e.g., memory area within a subscriber identity module or "SIM"). Following such access, parameters accessed from or derived from the SIM can be transmitted to an identity verification service. An identity verification service may compile, such as from the centralized repository, the complement of subscriber parameters based, at least in part, on the parameters accessed from or derived from the SIM of the communications device. The complement of subscriber parameters may be transmitted to the communications device via a communications network. Following receipt of the complement of subscriber parameters, fields of an online application for credit, for example, can be populated or pre-filled with subscriber-specific parameters. A complement of such subscriber parameters transmitted to a communications device may give rise to the device populating or pre-filling, for example, an application (such as a credit application), which may be displayed on the display of the communications device. Consequently, the subscriber can quickly, and with minimal effort, complete an application for credit, obtain an increase in credit, obtain an incentive from a participating credit-issuing, for example. Further, by pre-filling a complement of subscriber parameters on a display of a communications device, data entry errors, typographical errors, errors in punctuation and syntax, can be avoided so that a prospective account holder can be assured of a positive initial experience with a merchant or other institution. In particular embodiments, applications for

8

credit from a financial institution, merchant, or other type of institution may be accompanied by the institution providing an incentive bonus or an incentive award, for example, based on subscriber-unique parameters, as discussed further hereinbelow.

Some example methods, apparatuses, and/or articles of manufacture are disclosed herein that may be used, in whole or in part, to facilitate and/or support one or more operations and/or techniques that relate to transmitting a complement of subscriber parameters to a communications device. A complement of subscriber parameters transmitted to a communications device may enable the device to populate or pre-fill, for example, an application (such as a credit application), which may be displayed on the display of the communications device. Such techniques may be implemented in connection with a processor-equipped cellular mobile communications device communicating with one or more computing devices via the one or more communication networks (such as cellular communications networks) utilizing one or more communications protocols discussed herein.

In this context, the term "article" refers to an article of manufacture as well as a data or memory structure having instructions stored thereon. The communications device may be utilized to verify and/or authenticate a transacting party, such as a party interacting with a communications device to complete an application, such as an application for credit. Such electronic or on-line transactions, which may herein be referred to as simply "transactions," may involve transactions related to one or more financial accounts, such as accounts that relate to a line of credit, a communication device services account (e.g. associated with a mobile communications device), a bank account, a brokerage account, and so forth. In this context, a "transacting party" refers to an entity, such as an individual subscriber, who may attempt to engage in, and/or facilitate, an electronic or on-line transaction.

Although the discussion that follows relates to any type of account, as a non-limiting illustration, accounts related to mobile communications devices may be used for illustration. However, it is understood, of course, that claimed subject matter is intended to not be limited to examples provided primarily for purposes of illustration, since such examples may be oversimplified for purposes of comprehension, for example.

FIG. 1 is a diagram of a communications device situated within a cellular communications infrastructure, according to various embodiments. In FIG. 1 (embodiment 100) communications 102 may transmit radio signals to, and receive radio signals from, a wireless communications network. In an example, communications device 102 may communicate with a cellular communications network by transmitting wireless signals to, and/or receiving wireless signals from, a cellular transceiver 110, which may comprise a wireless base transceiver subsystem (BTS), a Node B or an evolved NodeB (eNodeB), over wireless communication link 123. Similarly, communications device 102 may transmit wireless signals to, and/or receive wireless signals from, local transceiver 115 over wireless communication link 125. A local transceiver 115 may comprise an access point (AP), femtocell, Home Base Station, small cell base station, Home Node B (HNB) or Home eNodeB (HeNB) and may provide access to a wireless local area network (WLAN, e.g., IEEE 802.11 network), a wireless personal area network (WPAN, e.g., Bluetooth® network) or a cellular network (e.g. an LTE network or other wireless wide area network, such as those discussed herein). Of course, it should be understood that

US 12,200,816 B2

9

these are merely examples of networks that may communicate with a communications device over a wireless link, and claimed subject matter is not limited in this respect. In particular embodiments, cellular transceiver **110**, local transceiver **115**, and satellite **114** represent touchpoints, which permit device **102** to interact with network **130**.

Examples of network technologies that may support wireless communication link **123** are GSM, Code Division Multiple Access (CDMA), Wideband CDMA (WCDMA), Long Term Evolution (LTE), High Rate Packet Data (HRPD). GSM, WCDMA and LTE are technologies defined by 3GPP. CDMA and HRPD are technologies defined by the 3rd Generation Partnership Project 2 (3GPP2). WCDMA is also part of the Universal Mobile Telecommunications System (UMTS) and may be supported by an HNB. Cellular transceivers **110** may comprise deployments of equipment providing subscriber access to a wireless telecommunication network for a service (e.g., under a service contract). In the embodiment of FIG. 1, a cellular transceiver **110** may perform functions of a cellular base station in servicing subscriber devices within a cell determined based, at least in part, on a range at which the cellular transceiver **110** is capable of providing access service. Examples of radio technologies that may support wireless communication link **125** are IEEE 802.11, BT and LTE.

In a particular implementation, cellular transceiver **110** and local transceiver **115** may communicate with server **140**, such as by way of network **130** via communication links **145**. Here, network **130** may comprise any combination of wired or wireless links and may include cellular transceiver **110** and/or local transceiver **115** and/or server **140**. In a particular implementation, network **130** may comprise Internet Protocol (IP) or other infrastructure capable of facilitating communication between communications device **102** at a call source and server **140** through local transceiver **115** or cellular transceiver **110**. In an embodiment, network **130** may also facilitate communication between communications device **102**, server **140** and a public switched telephone network, for example, through a suitable communications link. In another implementation, network **130** may comprise a cellular communication network infrastructure such as, for example, a base station controller or packet based or circuit based switching center (not shown) to facilitate cellular communication with communications device **102**. In a particular implementation, network **130** may comprise local area network (LAN) elements such as WiFi APs, routers and bridges and may, in such an instance, comprise links to gateway elements that provide access to wide area networks such as the Internet. In other implementations, network **130** may comprise a LAN and may or may not involve access to a wide area network but may not provide any such access (if supported) to communications device **102**. In some implementations, network **130** may comprise multiple networks (e.g., one or more wireless networks and/or the Internet). In one implementation, network **130** may include one or more serving gateways or Packet Data Network gateways. In addition, one or more of server **140** may comprise an E-SMLC, a Secure User Plane Location (SUPL) Location Platform (SLP), a SUPL Location Center (SLC), a SUPL Positioning Center (SPC), a Position Determining Entity (PDE) and/or a gateway mobile location center (GMLC), each of which may connect to one or more location retrieval functions (LRFs) and/or mobility management entities (MMEs) of network **130**.

In particular embodiments, communications between communications device **102** and cellular transmitter **110**, satellite **114**, local transceiver **115**, and so forth may occur

10

utilizing signals communicated across wireless communications channels. Accordingly, the term “signal” may refer to communications utilizing propagation of electromagnetic waves across wireless communications channels. Signals may be modulated to convey messages utilizing one or more techniques such as amplitude modulation, frequency modulation, binary phase shift keying (BPSK), quaternary phase shift keying (QPSK) along with numerous other modulation techniques, and claimed subject matter is not limited in this respect. Accordingly, as used herein, the term “messages” refers to parameters, such as binary signal states, which may be encoded in a signal using one or more of the above-identified modulation techniques.

In particular implementations, and as discussed below, communications device **102** may comprise circuitry and processing resources capable of obtaining location related measurements (e.g. for signals received from GPS or other Satellite Positioning System (SPS) satellites **114**), cellular transceiver **110** or local transceiver **115** and possibly computing a position fix or estimated location of communications device **102** based on these location related measurements. In some implementations, location related measurements obtained by communications device **102** may be transferred to a location server such as an enhanced serving mobile location center (E-SMLC) or SUPL location platform (SLP) (e.g. which may comprise a server, such as server **140**) after which the location server may estimate or determine an estimated location for communications device **102** based on the measurements. In the presently illustrated example, location related measurements obtained by communications device **102** may include measurements of signals (**124**) received from satellites belonging to an SPS or Global Navigation Satellite System (GNSS) such as GPS, GLONASS, Galileo or Beidou and/or may include measurements of signal strengths of signals utilized in wireless communication links **123** and/or **125** received from terrestrial transmitters fixed at known locations (e.g., such as cellular transceiver **110**).

Communications device **102** or a separate location server may obtain a location estimate for communications device **102** based on location related measurements using any one of several position methods such as, for example, GNSS, Assisted GNSS (A-GNSS), Advanced Forward Link Trilateration (AFLT), Observed Time Difference Of Arrival (OTDOA) or Enhanced Cell ID (E-CID) or combinations thereof. In some of these techniques (e.g. A-GNSS, AFLT and OTDOA), pseudoranges or timing differences may be measured at communications device **102** relative to three or more terrestrial transmitters fixed at known locations or relative to four or more satellites with accurately known orbital data, or combinations thereof, based at least in part, on pilots, positioning reference signals (PRS) or other positioning related signals transmitted by the transmitters or satellites and received at communications device **102**. Here, server **140** may be capable of providing positioning assistance data to communications device **102** including, for example, information regarding signals to be measured (e.g., signal timing), locations and identities of terrestrial transmitters and/or signal, timing and orbital information for GNSS satellites to facilitate positioning techniques such as A-GNSS, AFLT, OTDOA and E-CID. For example, server **140** may comprise an almanac to indicate locations and identities of cellular transceivers and/or local transceivers in a particular region or regions such as a particular venue, and may provide information descriptive of signals transmitted by a cellular base station or AP such as transmission power and signal timing. In the case of E-CID, communications

US 12,200,816 B2

11

device **102** may obtain measurements of signal strengths for signals received from cellular transceiver **110** and/or local transceiver **115** and/or may obtain a round trip signal propagation time (RTT) between communications device **102** and a cellular transceiver **110** or local transceiver **115**. A communications device **102** may use these measurements together with assistance data (e.g. terrestrial almanac data or GNSS satellite data such as GNSS Almanac and/or GNSS Ephemeris information) received from server **140** to determine a location estimate for communications device **102** or may transfer the measurements to server **140** to perform the same determination. A call from communications device **102** may be routed, based on the location of communications device **102**, and connected to the public switched telephone network, for example, via wireless communication link **123** and/or other communications links.

A communicating device at a call source (e.g., communications device **102** of FIG. **1**) may be referred to by any name corresponding to a cellphone, smartphone, laptop, tablet, PDA, tracking device or some other portable or movable device. Typically, though not necessarily, a communications device may support wireless communication such as using GSM, WCDMA, LTE, CDMA, HRPD, WiFi, BT, WiMax, etc. A communications device may also support wireless communication using a wireless LAN (WLAN), DSL or packet cable for example. A communications device may comprise a single entity or may comprise multiple entities such as in a personal area network where a subscriber may employ audio, video and/or data I/O devices and/or body sensors and a separate wireline or wireless modem. An estimate of a location of a communications device (e.g., communications device **102**) may be referred to as a location, location estimate, location fix, fix, position, position estimate or position fix, and may be geographic, thus providing location coordinates for the communications device (e.g., latitude and longitude) which may or may not include an altitude component (e.g., height above sea level, height above or depth below ground level, floor level or basement level).

The architecture of the cellular communications network described in relation to FIG. **1** may comprise a generic architecture that is capable of accommodating a variety of outdoor and indoor location solutions including the standard SUPL user plane location solution defined by the Open Mobile Alliance (OMA) and standard control plane location solutions defined by 3GPP and 3GPP2. For example, server **140** may function as (i) a SUPL location platform to support the SUPL location solution, (ii) an E-SMLC to support the 3GPP control plane location solution with LTE access on wireless communication link **123** or **125**, or (iii) a Stand-alone Serving Mobile Location Center (SAS) to support the 3GPP Control Plane Location solution for UMTS.

In view of the communications infrastructure shown and described in reference to FIG. **1**, more particular embodiments directed toward transmitting a complement of subscriber parameters to a communications device are discussed hereinbelow. Hence, FIG. **2** shows a subscriber interacting with an aspect of a cellular communications network, within a cellular communications infrastructure, to obtain a complement of subscriber parameters, according to an embodiment **200**. In the embodiment of FIG. **2**, subscriber **205** may be located at any point within cellular communications of cellular transceiver **110**. In the embodiment of FIG. **2**, subscriber **205** may be presently located in a department store, just as an example, within view of machine-readable layout **210**. Machine-readable layout **210** may be positioned, for example, near a human-readable placard, which may

12

advertise, just as an example, that a subscriber may obtain a credit card, for example, or other instrument, which may allow subscriber **205** to obtain a credit value (e.g., a credit limit) or other privileges at the department store. In particular embodiments, subscriber **205** may obtain any other type of numerical value (other than a credit value). Machine-readable layout **210** may represent a two-dimensional bar-code; however, in other embodiments, machine-readable layout **210** may represent any other type of machine-readable entity, such as a one-dimensional bar-code, or any other type of machine-recognizable or computer-recognizable pattern. Machine-readable layout **210** may be positioned nearby any other type of human-readable placard, for example, and claimed subject matter is not limited in this respect. In other instances, machine-readable layout **210** comprises a stand-alone machine-readable layout, presented on a placard, on the page of the magazine, or any other location readable by a camera device of communications device **102**.

As shown in FIG. **2**, subscriber **205** may situate communications device **102** so as to permit viewing and/or image capture of machine-readable layout **210** utilizing a camera of communications device **102**. In the embodiment of FIG. **2**, machine-readable layout **210** may be utilized in conjunction with a human-readable placard, which indicates to subscribers (e.g., subscriber **205**), that a subscriber may initiate application for a credit account, for example, beginning with capturing an image of machine-readable layout **210**, or by otherwise bringing machine-readable layout **210** into view of a camera of communications device **102**. In the embodiment of FIG. **2**, communications device **102** may execute a computer process, which may, in response to capturing or viewing an image of machine-readable layout **210**, connect with a uniform resource locator (URL) via a browser operating on communications device **102**. In some instances, the URL may correspond to a bank or other type of financial institution, which may permit subscriber **205** to complete an application for credit.

In addition to a browser program instructing communications device **102** to connect, via a browser, to a website corresponding to a bank or other type of financial institution, a computer process executing on device **102** may access a memory storage device, such as a SIM card, to obtain an identifier of the communications device. In particular embodiments, an identifier of a communications device may comprise a subscriber account identifier (e.g., a telephone number), International Mobile Subscriber Identifier (IMSI), an International Mobile Electronic Identifier (IMEI), or a Mobile Station International Subscriber Directory Number (MSISDN), or any combination thereof. An identifier of a communications device **102** may be transmitted to cellular transceiver **110** along with a request to initiate completion of a credit application, or an application to enter into any other type of agreement with, for example, a bank or financial institution.

As shown in FIG. **2**, an identifier may be conveyed through one or more communication links, such as indicated by network **145**. An identifier may be provided to client **225**, which may correspond to a financial institution, such as a bank or any other institution. Responsive to receipt of an identifier, client **225** may query identity verifier **228**, which may, in turn, access device database **230**. In the embodiment of FIG. **2**, device database **230** may include records of various deterministic events, such as records of number porting of communications device **102**, records related to removal/replacement of a SIM, instances of password resets of a communications device, records of communications device tenure, and so forth. Device database **230** may

US 12,200,816 B2

13

include records that relate to other aspects of the behavior of subscriber **205** with respect to a communications device, and claimed subject matter is not limited in this respect. In addition to various historical events stored within device database **230**, the database may include records referring to the “velocity” of a historical event, which may represent a rate or a frequency of occurrence of an online or off-line deterministic event with respect to time. For example, a subscriber’s phone number-porting events may occur with a velocity of one event per one-year period. In other examples, deterministic events having a velocity aspect may refer to the rate (perhaps in occurrences per year) that a subscriber removes/replaces a SIM, replaces a communications device, resets or obtains a password, or may relate to any other online or off-line deterministic event. Further, various historical events stored within device database **230**, with respect to communications device **102**, may additionally pertain to browsing habits of subscriber **205**, shopping habits of subscriber **205**, and so forth.

In response to receipt of an identifier from communications device **102**, via cellular transceiver **110**, network **145**, and client **225**, identity verifier **228** may transmit a complement of subscriber parameters to client **225**. In particular embodiments, identity verifier **228** may transmit a subscriber name, physical address (e.g., street address, city, town, municipality, ZIP Code, etc.) along with other subscriber parameters, which may include Social Security number. In other embodiments, identity verifier **228** may additionally transmit past physical addresses, current/past employer parameters, and a host of subscriber parameters, and claimed subject matter is not limited in this respect.

Following receipt of a complement of subscriber parameters, client **225** may transmit a request to communications device **102** for one or more additional identifying parameters. For example, an identifying parameter may comprise a Social Security number, or portion thereof (e.g., last four digits) for display to subscriber **205**. Responsive to receipt of such request, subscriber **205** may enter the one or more additional identifying parameters (e.g., last four digits of Social Security number), which may operate to provide verification and/or authentication of subscriber **205**. Following subscriber **205** entering the one or more additional identifying parameters into a user interface of communications device **102**, the one or more additional identifying parameters may be transmitted, via communications link **123**, cellular transceiver **110**, and network **145** to client **225**. Responsive to receipt of the one or more additional identifying parameters, client **225** may determine that subscriber **205** is the authentic (e.g., verified) owner of communications device **102**, and/or that communications **102** is co-located with subscriber **205**. Client **225** may make additional determinations based on the one or more additional identifying parameters, and claimed subject matter is not limited in this respect.

Client **225** may then transmit a complement of subscriber parameters for display utilizing a user interface of communications device **102**. Accordingly, subscriber **205** may need only double check and/or verify that an application, such as an application for credit, has been pre-filled/populated by the parameters transmitted by client **225**. At such point, subscriber **205** may perhaps depress a “submit” selector, which may, in turn, convey the pre-filled/populated credit application to client **225**.

It may be appreciated that in the embodiment of FIG. 2, to complete an application, such as an application for credit, for example, subscriber **205** need only minimally interact with a communications device **102**. For example, to initiate

14

a process to complete an application, subscriber **205** may capture an image of machine-readable layout **210**, which may correspond to a quick response (QR) code. Responsive to capture of the machine-readable layout, a memory device of communications device **102** may be queried, resulting in an identifier of device **102** being transmitted to cellular transceiver **110**. In particular instances, transmission of an identifier of communications device **102** may be accompanied with an indication that subscriber **205** wishes to complete an application, such as a credit application. Following determination of parameters specific to subscriber **205**, client **225** may request, at least in certain instances, a single parameter to be verified by subscriber **205** (e.g., last four digits of Social Security number). Responsive to confirmation of the single parameter by subscriber **205**, a credit application may be pre-filled (e.g., pre-populated) with a complement of subscriber-specific parameters. In particular embodiments, subscriber **205** may simply select to “submit” the pre-filled credit application. Accordingly, in such a scenario, an application, such as a credit application, can be completed responsive to actuating six (6) selectors of a user interface of a cellular communications device, such as (selection 1) actuating a camera to capture an image of layout **210**, (selections 2-5) entering four digits of a Social Security number, followed by (selection 6) actuating a “submit” selector.

Although not specifically discussed in reference to FIG. 2, following an identity verification process, such as involving identity verifier **228**, the eligibility of subscriber **205** for pre-fill of a credit application, for example, may be determined. In an example, responsive to completion of an authentication process performed by an identity verifier, a complement of subscriber parameters may be transmitted to a communications device. Identity verification may take place utilizing one or more parameters stored in (or derived from) a SIM of a communications device, or may take place utilizing a subscriber’s verified telephone number, a subscriber’s persistent identifier, or utilizing any other type of subscriber account identification number. Alternatively, authentication of a communications device may take place responsive to an identity verifier transmitting a one-time short messaging system (SMS) passcode to a communications device. In such instances, an identity verifier may determine whether a subscriber is eligible for an automatic (e.g., without subscriber input) pre-fill of a form such as e-commerce checkout, digital sign-up, or an application for a service. In addition to determining whether a particular subscriber is eligible for pre-fill of a credit application, an identity verifier, cooperating with a computing resource of a credit issuer, may transmit one or more incentives to a subscriber, so as to entice the subscriber to complete and submit a credit application. In some instances, such incentives may be based, at least in part, on a subscriber’s taxable income, discretionary income, demographics, credit history, credit score, spending history with a particular merchant, lifetime spending potential with a merchant, etc., and claimed subject matter is intended to embrace all such factors that may influence an incentive.

In particular embodiments, eligibility may be determined utilizing flexible, client-defined rules and/or guidelines. For example, eligibility for pre-fill of a form may be determined utilizing (but not limited to) criteria such as data attributes, which, for example, may include name/address, Social Security number, date-of-birth, household ID (e.g., last name of perhaps multiple subscribers living at a common physical address, etc. Eligibility for pre-fill of a form may also be dependent upon reputational scoring, which may

US 12,200,816 B2

15

correspond to the reputation of communications device **102** and/or subscriber **205**. For example, a trustworthiness score or other measure of trustworthiness may be utilized in computing reputational scoring. Eligibility for pre-fill of a form may also be dependent upon demographic attributes of a subscriber, such as the subscriber's chronological age, ZIP Code of residence, taxable income, and so forth. Eligibility for pre-fill of a form may also be dependent upon parameters related to a communication services provider account, an account type, a device and/or subscriber account identifier (e.g., telephone number) tenure, trustworthiness score, etc. Eligibility for pre-fill of a form may also be dependent upon industry-specific attributes of a subscriber. For example, in an e-commerce environment, creating an account may involve, perhaps exclusively, parameters such as a subscriber name, address, phone number (or other type of subscriber account identifier, persistent identifier, subscriber-unique identifier, and so forth). In particular regulated industries, such as financial services or communication services carriers, creating an account may involve entry of parameters such as name, address, phone number (or other type of subscriber account identifier) Social Security number, date of birth, etc. Such parameters may fulfill know your customer (KYC) regulatory requirements for new account origination. Eligibility for pre-fill of a form may also utilize industry-specific scoring or computed metrics, which may include a lifetime value (e.g., covering a period of one year, two years, three years, etc.) based upon past transactional and/or purchase history. Such industry-specific scoring may include financial scoring such as credit-worthiness, whether at an individual level, and anonymized individual level, or at and anonymized aggregate level. Such industry-specific scoring may include behavioral interaction such as repeat visits, community engagement, or client-derived reputation scores. Eligibility for pre-fill of a form may include incentive scoring, which may relate to client-specified attributes and/or scoring, such as lifetime value or creditworthiness, which may result in client-specified incentives to be displayed with pre-fill or an automatic (e.g., without subscriber input) fill selector. In particular embodiments, providing such incentives may encourage a subscriber to complete, for example, a credit application in an e-commerce checkout or a digital sign-up application. Eligibility for pre-fill of a form may include geographic scoring, which may relate to whether a phone is currently located within a client-specific radius (e.g., 1 km, 5 km, 10 km, 25 km, 50 km, etc.) of a physical address associated with a communication services account or physical address (or sharing the same IP address as associated device such as a laptop, tablet, desktop or personal computer, smart TV, etc.

In particular embodiments, in response to determination of eligibility, a number of outcomes may result:

- (1) Responsive to a subscriber being determined to be eligible, the pre-fill or auto-fill (e.g., without subscriber input) selector may be presented in a user interface of a communications device as an option to complete the form such as e-commerce checkout, digital sign-up, or application. Following selection of the selector, an identity verifier may fetch subscriber parameters from communication services providers, credit bureaus, and/or prepaid processors, etc., so as to complete a credit account application on behalf of the consumer.
- (2) Responsive to a determination that a subscriber may not be eligible for pre-fill, there may be little or negligible interruption to the subscriber experience. In such a scenario, a pre-fill or auto-fill selector may not be displayed (or may be displayed as a grayed-out

16

selection) in which the subscriber continues a checkout, digital sign-up, or applications.

- (3) Responsive to a determination that a subscriber has been considered to be eligible, but does not choose a pre-fill or auto-fill option, the potential subscriber may choose to manually complete a form such as e-commerce checkout, digital sign-up, or application, whether the potential subscriber is eligible for the pre-fill experience. In such instances, an identity verifier may verify manually-entered parameters utilizing identity verification, in which parameters may be obtained from communication services providers, credit bureaus, and/or prepaid processors. In such instances, matching algorithms may be applied to parameters obtained utilizing, for example, fuzzy matching, gender, inversions, old but valid addresses, householding for family plans etc., and claimed subject matter is intended to embrace all such approaches.

In particular embodiments, following completion of the form, and following subsequent processing of the form, a client (e.g., an identity verifier) may utilize eligibility criteria to further simplify application processes. Such simplifications may be utilized by financial services institutions to provide access to a predetermined line of credit at account origination, a payment network adding a newly-obtained credit card directly to a mobile wallet for immediate use, a retailer offering an incentive for first time use of a new store private label or co-brand credit card, a mobile communication services provider offering a free or reduced-fee trial of new services such as music subscription, satellite radio, etc., and claimed subject matter is not limited in this respect.

As previously noted, client-specified incentives may be displayed with pre-fill or with an automatic fill selector (e.g., without user interface), which may encourage a subscriber to complete a credit application, for example. In particular embodiments, a client-specified incentive may include a numerical value corresponding to a predetermined bonus amount, for example, which may be given or awarded to the subscriber in response to the subscriber opening a credit account. A numerical value corresponding to a predetermined bonus amount may be awarded to a subscriber based, at least in part, on reported taxable income (or an estimate of taxable income), a subscriber's reported discretionary income (or an estimate of discretionary income), a measure of a subscriber's standing as an influencer of a social network (e.g., social network activity, number of followers, number of posts, etc.), marital status, Fair Isaac Corporation (FICO) score, and/or a measure of the subscriber's past spending history (or history of other engagements) with a certain merchant or with an affiliated merchant, an estimate of a subscriber's potential future (e.g., lifetime) spending with a certain merchant, a record of a subscriber having credit accounts with certain banks and/or lending institutions, etc. A numerical value of predetermined bonus award amount may be based on other factors and/or characteristics of a subscriber, and claimed subject matter is not limited in this respect.

FIG. 3 shows a message flow diagram in a method of transmitting a complement of subscriber parameters to a communications device, according to an embodiment **300**. The diagram of FIG. 3 begins with subscriber **205** interacting with a communications device, such as device **102** of FIG. 2, so as to access an identifier on a SIM of device **102**. As described in FIG. 2, an identifier stored on a SIM may be accessed responsive to a camera of communications device **102** capturing an image of machine-readable layout **210**. As mentioned with respect to FIG. 2, capture of machine-

US 12,200,816 B2

17

readable layout **210** may permit communications device **102** to connect (e.g., via a browser-based session) with a bank or other type of financial institution to permit subscriber **205** to complete an application for credit, apply for increased credit, or initiate any other application for a privilege to be granted (e.g., borrowing funds, obtaining a line of credit, etc.).

Responsive to identifier **305** being accessed from a SIM of a communications device, perhaps in response to subscriber **205** capturing an image of machine-readable layout **210**, identifier **305** may be conveyed via link **123** (of FIG. 2) through cellular transceiver **110**, and through network **130**. Identifier **305** may then be presented to client **225**, which may represent a bank, credit union, or other type of institution capable of providing loans, lines of credit, access to privileged/premium content (e.g., for a fee), etc. Client **225** may pass identifier **305** to identity verifier **228**. Identity verifier **228** may, in turn, access device database **230**, which may provide complement **310** (e.g., name, current/past addresses, current/past employers, phone number, and so forth). Complement **310** may additionally include one or more additional identifying parameters for confirmation/verification by subscriber **205**. Complement **310** may be stored, at least temporarily, within a memory structure at client **225**.

In the embodiment of FIG. 3, device database **230** may additionally supply a trustworthiness score with respect to communications device **102**. In particular embodiments, a trustworthiness score may be computed in response to determining events, which may occur with respect to communications device **102**. Such events may correspond to a length of time that a subscriber **205** has been in possession of communications device **102** (e.g., device tenure), whether communications device **102** has been recently ported (e.g., involving a telephone number or other subscriber account identifier) from a first communications service carrier to a second communications service carrier, whether a one-time password has been utilized to reset account parameters accessed by communications device **102**, as well as any number of additional online or off-line events involving device **102**. A trustworthiness score may be computed utilizing a history of other deterministic events, and claimed subject matter is not limited in this respect.

Client **225** may pass additional parameters request **315**, via network **130**, to subscriber **205**. In the embodiment of FIG. 3, an additional parameters request may correspond to a parameter perhaps known only to a select few individuals, such as subscriber **205**. Such parameters may include a portion of a Social Security number (e.g., the last four digits) or any other parameter, such as mother's maiden name, name of childhood friend, city of birth, or any other parameter generally not known to others, and claimed subject matter is intended to embrace all such parameters. Responsive to receipt of a request for additional data, which may be displayed via a display of (or coupled to) communications device **102**, subscriber **205** may provide requested parameters **320**. Requested parameters **320** may propagate through network **130** for receipt by client **225**. Responsive to receipt of the requested parameters **320**, client **225** may compare requested parameters **320** with a parameter known only to subscriber **205**, for example, to determine if a match exists. Responsive to detection of a match, client **225** may determine that subscriber **205** has been authenticated. Accordingly, client **225** may transmit a complement of subscriber parameters (e.g. subscriber parameter complement **330**) to communications device **102** for review by subscriber **205**.

18

Responsive to receipt of the complement of subscriber parameters at communications device **102**, device **102** may pre-fill (populate) fields of an application or other type of form, perhaps for use in connection with obtaining credit by subscriber **205**. Subscriber **205** may merely verify the entries of a pre-filled form displayed via a display of communications device **102**. Subscriber **205** may then actuate a "submit" selector, which may operate to convey a completed credit application (e.g., completed application **340**), for example, via network **130** to client **225**. Upon receipt of a completed credit application, for example, client **225** may compute a credit amount and/or compute any other amount or parameter, and forward such amount to subscriber **205** for display on a display of communications device **102**.

Credit amount **350** may be computed based, at least in part, on score **312** computed by (or in cooperation with) identity verifier **228** responsive to accessing device database **230**. In particular embodiments, responsive to device database **230** indicating that communications device **102** can be considered to be relatively trustworthy, such as following a determination that fraudulent events have not occurred in connection with device **102**, score **312** may comprise a relatively high number. Conversely, responsive to device database **230** indicating that communications device **102** can be considered relatively untrustworthy, such as following a determination that fraudulent events have occurred in connection with device **102**, score **312** may comprise a relatively low number.

FIG. 4A shows a communications device displaying an interface to accept a complement of subscriber parameters, according to an embodiment **400**. As depicted in FIG. 4A, communications device **102** comprises image capture device **402**, which may correspond to a camera, for example. In an embodiment, a subscriber, such as subscriber **205** of FIG. 2, may position machine-readable layout **210** into the field-of-view of image capture device **402**. Responsive to machine-readable layout **210** being positioned within the field-of-view of image capture device **402**, a process (e.g., an application program interface) executing on a processor of communications device **102** may be directed to connect to a URL for the purpose of initiating a credit application. In alternative embodiments, communications device **102** may be directed to connect to a URL for the purpose of initiating any other type of application, such as an application to upgrade credit (e.g., increase a credit value or credit limit), an application to obtain premium content, or any other type of application, and claimed subject matter is not limited in this respect.

Following communications device **102** being connected to a URL to facilitate initiation of a browser-based session, a computer program executing on a processor of communications device **102** may access an identifier stored on SIM **403**. In some embodiments, an identifier stored on SIM **403** may comprise a subscriber account identifier (e.g., a telephone number), International Mobile Subscriber Identifier (IMSI), an International Mobile Electronic Identifier (IMEI), or a Mobile Station International Subscriber Directory Number (MSISDN), or any combination thereof. The identifier may be conveyed through a cellular communications network, such as described with reference to FIG. 1, to a client (e.g., client **225** of FIG. 2), which may correspond to a bank, financial clearinghouse, or other type of institution involved in extending credit, providing premium content, or fighting other types of privileges to subscribers. In turn, client **225** may contact an identity verification service (e.g., identity verifier **228**), who may access a device database (e.g., device database **230**) to obtain parameters specific to

US 12,200,816 B2

19

the subscriber **205** co-located with communications device **102**. In some embodiments, device database **230** may also provide a trustworthiness score or other measure of trustworthiness, with respect to communications device **102**, based, at least in part, on records of historical events involving communications device **102**. Such records may include instances of reassignment of subscriber account identifiers (e.g., telephone numbers) from a first communications service carrier to a second communications service carrier, tenure of device **102**, instances of password resets with respect to device **102**, removal or replacement of a SIM (e.g., SIM **403**), along with other behavioral aspects with respect to device **102**.

FIG. **4B** shows a communications device displaying a user interface into which a complement of subscriber parameters has been pre-filled into the user interface, according to an embodiment. In response to a client (e.g., client **225** of FIG. **2**) determining a complement of subscriber-specific parameters corresponding to an identifier accessed from SIM **403**, a blank application form, such as indicated in FIG. **4A**, may be pre-filled with subscriber-specific parameters. Such parameters may include subscriber's full name, past and/or present addresses, past and/or present employers, and other specific parameters. In particular embodiments, pre-filled application **405** may be displayed on a display of communications device **102** within seconds (e.g., 10 seconds, 20 seconds, 30 seconds, 60 seconds, 90 seconds) of subscriber **205** capturing an image of machine-readable layout **210**. In particular embodiments, an intermediate operation, not explicitly indicated in FIGS. **4A/4B** may involve subscriber **205** verifying one or more additional parameters, such as the last four digits of a Social Security number (just to name an example) as an approach toward validating and/or a verifying the identity of subscriber **205**, prior to conveying the complement of subscriber-specific parameters indicated as pre-filled application **405**. In particular embodiments, a subscriber may actuate submit selector **407**, so as to submit the completed credit application to a lending institution or its representative.

FIG. **5** shows a process of transmitting a complement of subscriber parameters to a device, according to an embodiment **500**. It should be noted that the disclosed embodiments, such as the embodiment of FIG. **5**, are intended to embrace numerous variations, including methods that may include actions in addition to those depicted in the figures, actions performed in an order different than those depicted in the figures, as well as methods including fewer steps than those depicted. The method of FIG. **5** begins at **505**, which includes obtaining, from a communications device (e.g., a mobile communications device), an identifier of the communications device transmitted via a communications network. **505** may involve a subscriber (such as subscriber **205** of FIG. **2**) capturing an image of a machine-readable layout in order to initiate an application for credit, or an application for any other type of privilege including upgrading an existing line of credit, obtaining access to privileged content, etc. attempting to initiate an electronic or digital transaction, such as an electronic financial transaction, by contacting a bank, brokerage, or other institution. **505** may additionally include a communications device transmitting an identifier, such as accessed from a SIM of a communications device.

At **510**, responsive to a client (such as client **225** of FIG. **2**) obtaining name, address, and other parameters of subscriber **205**, a client may transmit, to the communications network, a request for one or more parameters unique to a subscriber of a communications network (e.g., subscriber **205**). Such parameters may include a date of birth, Social

20

Security number, mother's maiden name, etc. At **515**, in response to receiving a response from subscriber **205** for one or more additional parameters, a client, such as client **225** of FIG. **2**, may determine if a match exists between the one or more additional parameters and the name, address, and other parameters obtained from an identity verification service (e.g., identity verifier **228** of FIG. **2**). **515** may include processing of signals indicative of the requested one or more parameters provided in response to the subscriber entering the one or more parameters into a graphical user interface of the communications device. For example, at **515**, the last four digits of a Social Security number accessed from device database **230** may be compared with the last four digits supplied by a subscriber **205** in response to the request for one or more parameters (such as described in reference to **510**).

At **520**, responsive to a match existing between the last four digits of a Social Security number (for example) provided by a subscriber and (again, for example) the last four digits of a Social Security number provided by a device database, a client may transmit, to the communications device, one or more signals to provide a complement of subscriber parameters. A complement of subscriber parameters may be utilized to pre-fill an application form, or other type of form, displayed on a display of a communications device located with subscriber **205**.

FIG. **6** is a diagram showing a computing environment, according to an embodiment **600**. In the embodiment of FIG. **6**, first and third devices **602** and **606** may be capable of rendering a graphical user interface (GUI) for a network device, such as server device **140** of FIG. **1**, so that a subscriber utilizing a communications device (e.g., a mobile communications device) may engage in system use. Device **604** may potentially serve a similar function in this illustration. Likewise, in FIG. **6**, computing device **602** ('first device' in FIG. **6**) may interface with computing device **604** ('second device' in FIG. **6**), which may, for example, also comprise features of a client computing device and/or a server computing device, in an embodiment. Processor (e.g., processing device) **620** and memory **622**, which may comprise primary memory **624** and secondary memory **626**, may communicate by way of a communication interface **630**, for example. The term "computing device," in the context of the present patent application, refers to a system and/or a device, such as a computing apparatus that includes a capability to process (e.g., perform computations) and/or store digital content, such as electronic files, electronic documents, measurements, text, images, video, audio, etc. in the form of signals and/or states. Thus, a computing device, in the context of the present patent application, may comprise hardware, software, firmware, or any combination thereof (other than software per se). Computing device **604**, as depicted in FIG. **6**, is merely one example, and claimed subject matter is not limited in scope to this particular example.

In FIG. **6**, computing device **602** may provide one or more sources of executable computer instructions in the form of physical states and/or signals (e.g., stored in memory states), for example. Computing device **602** may communicate with computing device **604** by way of a network connection, such as via network **608**, for example. As previously mentioned, a connection, while physical, may be virtual while not necessarily being tangible. Although computing device **604** of FIG. **6** shows various tangible, physical components, claimed subject matter is not limited to a computing devices having only these tangible components as other implementations and/or embodiments may include alternative

US 12,200,816 B2

21

arrangements that may comprise additional tangible components or fewer tangible components, for example, that function differently while achieving similar results. Rather, examples are provided merely as illustrations. It is not intended that claimed subject matter be limited in scope to illustrative examples.

Memory **622** may comprise any non-transitory storage mechanism. Memory **622** may comprise, for example, primary memory **624** and secondary memory **626**, additional memory circuits, mechanisms, or combinations thereof may be used. Memory **622** may comprise, for example, random access memory, read only memory, etc., such as in the form of one or more storage devices and/or systems, such as, for example, a disk drive including an optical disc drive, a tape drive, a solid-state memory drive, etc., just to name a few examples.

Memory **622** may comprise one or more articles utilized to store a program of executable computer instructions. For example, processor **620** may fetch executable instructions from memory and proceed to execute the fetched instructions. Memory **622** may also comprise a memory controller for accessing device readable-medium **640** that may carry and/or make accessible digital content, which may include code, and/or instructions, for example, executable by processor **620** and/or some other device, such as a controller, as one example, capable of executing computer instructions, for example. Under direction of processor **620**, a non-transitory memory, such as memory cells storing physical states (e.g., memory states), comprising, for example, a program of executable computer instructions, may be executed by processor **620** and able to generate signals to be communicated via a network, for example, as previously described. Generated signals may also be stored in memory, also previously suggested.

Memory **622** may store electronic files and/or electronic documents, such as relating to one or more subscribers, and may also comprise a machine-readable medium that may carry and/or make accessible content, including code and/or instructions, for example, executable by processor **620** and/or some other device, such as a controller, as one example, capable of executing computer instructions, for example. As previously mentioned, the term electronic file and/or the term electronic document are used throughout this document to refer to a set of stored memory states and/or a set of physical signals associated in a manner so as to thereby form an electronic file and/or an electronic document. That is, it is not meant to implicitly reference a particular syntax, format and/or approach used, for example, with respect to a set of associated memory states and/or a set of associated physical signals. It is further noted an association of memory states, for example, may be in a logical sense and not necessarily in a tangible, physical sense. Thus, although signal and/or state components of an electronic file and/or electronic document, are to be associated logically, storage thereof, for example, may reside in one or more different places in a tangible, physical memory, in an embodiment.

Algorithmic descriptions and/or symbolic representations are examples of techniques used by those of ordinary skill in the signal processing and/or related arts to convey the substance of their work to others skilled in the art. An algorithm is, in the context of the present patent application, and generally, is considered to be a self-consistent sequence of operations and/or similar signal processing leading to a desired result. In the context of the present patent application, operations and/or processing involve physical manipulation of physical quantities. Typically, although not necessarily, such quantities may take the form of electrical and/or

22

magnetic signals and/or states capable of being stored, transferred, combined, compared, processed and/or otherwise manipulated, for example, as electronic signals and/or states making up components of various forms of digital content, such as signal measurements, text, images, video, audio, etc.

Processor **620** may comprise one or more circuits, such as digital circuits, to perform at least a portion of a computing procedure and/or process. By way of example, but not limitation, processor **620** may comprise one or more processors, such as controllers, micro-processors, micro-controllers, application specific integrated circuits, digital signal processors, programmable logic devices, field programmable gate arrays, the like, or any combination thereof. In various implementations and/or embodiments, processor **620** may perform signal processing, typically substantially in accordance with fetched executable computer instructions, such as to manipulate signals and/or states, to construct signals and/or states, etc., with signals and/or states generated in such a manner to be communicated and/or stored in memory, for example.

FIG. **6** also illustrates device **604** as including a component **632** operable with input/output devices, and communication bus **615**, for example, so that signals and/or states may be appropriately communicated between devices, such as device **604** and an input device and/or device **604** and an output device. A subscriber may make use of an input device, such as a computer mouse, stylus, track ball, keyboard, and/or any other similar device capable of receiving subscriber actions and/or motions as input signals. Likewise, for a device having speech to text capability, a subscriber may speak to generate input signals. Likewise, a subscriber may make use of an output device, such as a display, a printer, etc., and/or any other device capable of providing signals and/or generating stimuli for a subscriber, such as visual stimuli, audio stimuli and/or other similar stimuli.

FIG. **7** shows a flowchart for a process of transmitting a complement of subscriber parameters to a communications device, according to an embodiment **700**. The process of FIG. **7** may begin at **705**, which may include a subscriber) visiting an application page of a merchant or financial institution affiliated with the merchant. **705** may involve a subscriber locating a machine-readable layout (e.g., machine-readable layout **210**) within the field-of-view of an imaging device **402** (e.g., a camera) of communications device **102**. The process may proceed with an instant authentication subprocess (1) in which a subscriber may be determined to be eligible and a pre-fill or auto-filled selector is presented in a user interface of communications device **102** as in **715**. Following selection of a selector to pre-fill or auto-fill an application, pre-filled application **405** may be displayed on a display of communications device **102**.

Responsive to a determination that a subscriber may not be eligible for pre-fill or auto-fill, a pre-fill or auto-fill selector may not be displayed. In this instance, **715** may invoke a manual process (e.g., authentication (2)). Also at **715**, responsive to a determination that a potential subscriber is eligible for pre-fill or auto-fill, but chooses to manually complete and e-commerce checkout, digital sign-up or completion of a credit application, an identity verifier may verify manually-entered parameters utilizing identity verification. In such a scenario (e.g., authentication (3)), parameters may be obtained from communication services providers, credit bureaus, and/or prepaid processors. In such instances, matching algorithms may be applied to parameters obtained utilizing, for example, fuzzy matching, gen-

US 12,200,816 B2

23

der, inversions, old but valid addresses, householding for family plans etc., and claimed subject matter is intended to embrace all such approaches.

In a fallback subprocess, one or more alternative authentication methods **720** may be performed. In a particular embodiment, as part of customer assessment **725** the subscriber may be prompted to enter a telephone number or other type of subscriber account identifier. In response to receiving a subscriber account identifier (e.g., a telephone number) an identity verifier (e.g. identity verifier **228** of FIG. **2**) may compute or obtain a trustworthiness measure (e.g., a trust score), such as at **725**. Just as an example, in response to the computed or obtained trust score being greater than a predetermined value, a link may be conveyed, such as via SMS. Responsive to receipt of an SMS message, a subscriber may select the link, resulting in verification of the communications device. Continuing with an example, in response to the computed or obtained trust score being less than the predetermined value, the subscriber may be directed to complete an application for credit (for example) utilizing a standard (e.g., manual entry) treatment or process.

Upon receipt of an authentication request, a verified mobile telephone number (or other type of subscriber account identifier) may be utilized as part of a real-time process to verify and/or authenticate a subscriber. Authentication may be achieved via direct authentication utilizing parameters stored in, for example, device database **230**, or via transmission of a one-time short messaging system (SMS) transmission of a passcode, and/or via transmission of a one-time passcode from, for example, a call center through a telephone call (e.g., a voice call) to a particular phone number. To ensure the security of such processes, such as described in reference to FIG. **2**, a communications device and/or other ancillary devices may participate in an authentication process. The authentication process may make use of a temporary, time-limited (e.g., 1 second, 1 minute, 1 hour, 1 day, etc.) identifier unique to a current authentication event. Such identifiers may include, but are not limited to, WIFI IP addresses, virtual private network (VPN) identifiers (e.g., VPN-IDs, etc.), and/or any other ancillary or like identifiers (e.g., a browser cookie, a browser fingerprint, etc.) generated during an authentication subprocess. In some embodiments, such identifiers may be passed between, for example, an identity verifier and a mobile device so as to maintain a linkage between individual steps of an authentication process. Use of such identifiers may prevent or at least reduce the occurrence of third parties submitting fraudulent requests in connection with (or attempting to intervene within) an authentication process or event. If a request is made either with a fraudulent, incorrect identifier or after the expiration of the identifier (e.g., 1 second, 1 minute, 1 hour, 1 day, etc.), the process, such as described in reference to FIG. **2**, may be terminated. Termination of an authentication process may be followed by a fresh (e.g., repeated) authentication request. If repeated requests (e.g., 2 requests, 3 requests, 5 requests, etc.) are made with fraudulent, incorrect, and/or expired identifiers unique to the current authentication event, within a certain time frame (e.g., 1 second, 1 minute, 1 hour, 1 day, etc.), the process, such as described in reference to FIG. **2**, may be terminated and the subscriber may be temporarily blocked (e.g., 1 hour, 1 day, 1 month, 1 year, etc.) from initiating further authentication events.

In response to an assessment (such as customer assessment **725**) indicating that a subscriber (such as subscriber **205**) is eligible for pre-fill (as described with respect to **710**) a prompt (such as at **730**) for the subscriber to enter

24

additional parameters, such as, for example, an identifier comprising the last four digits of a Social Security number, may be conveyed to the subscriber's communications device. Responsive to correct entry of the subscriber identifier (e.g., the last four digits of a Social Security number), which matches the last four digits of a Social Security number stored, for example, in device database **230** of FIG. **2**, a complement of parameters may be transmitted to the communications device in the subscriber's possession (e.g., at **740**). In particular embodiments up to 3 attempts (e.g., retries) to enter a parameter, such as the last four digits of a Social Security number, may be permitted. The complement of parameters may then be pre-filled into a form in the application process may be completed (e.g., at **755**). The subscriber's customer ID, subscriber account identifier, or any other identifying number, such as a persistent identifier other than a telephone number, may undergo data processing (e.g., at **760**) for entry into a database (e.g. **765**) for future reference (e.g., at **760**).

In particular embodiments, in response to determining that a subscriber is ineligible for pre-fill of, for example, an application for credit, the subscriber may be presented with a blank application form for manual entry (e.g., at **735**). Responsive to the subscriber successfully (manually) entering a complement of parameters (e.g., non-pre-fill process **745**), such as phone number and personally identifiable information, an identity verification subprocess may be performed. Responsive to successful completion of identity verification based on manually-entered subscriber parameters, personally identifiable information may be utilized to complete the application process, the results of which may be stored in to a customer or subscriber database. A non-pre-fill process (e.g., at **745**) may be invoked responsive failure of an identity verification process (e.g., at **750**). A non-pre-fill process (e.g., at **745**) may involve use of paper credit applications, for example, transmitted to an issuing bank or other financial institution, utilizing a manually-completed form.

In addition to apparatuses and approaches toward transmitting a complement of subscriber-unique parameters to a communications device, the foregoing provides illustrative examples of accounts in which a risk of fraud and/or unauthorized actions may exist. In accordance with such illustrative examples, a subscriber may attempt to access a bank account via a voice call, a web browser, or by utilizing a computer process executing on a communications device, for example, which may permit the subscriber to complete an application for credit. Thus, a bank, lender, brokerage firm, or any other type of financial institution, in response to the attempt to access the bank account, may employ an application programming interface (API) substantially compatible and/or substantially compliant with HTTP and/or HTTPS, including versions now known and/or to be later developed, and/or another suitable protocol (e.g., now known and/or to later be developed). In the foregoing example, a subscriber may seek to take one or more actions with respect to an account, such as, for example, establishing an account, updating a credit value (e.g., credit limit) for an account, transferring funds, viewing a history of electronic or digital transactions, updating privileged content and/or parameters, etc. Further, a bank, lender,

Thus, as suggested, a user may seek to obtain and/or access, for example, an online account. A third party, such as those who may provide such an account, may seek to provide an appropriate level of access control for such reasons as maintaining confidentiality of customer or subscriber information. In an example, a software company

US 12,200,816 B2

25

and/or product, such as a developer of tax-preparation software products, permit individual subscriber accounts to be established. It may also be appreciated that similar protections may be instituted in which confidentiality may not be an aspect. For example, with regard to management of certain types of privileged content and/or parameters, a user may seek to access such content in connection with an online subscription to a major newspaper. In another instance, a user may desire to access privileged content and/or parameters, whether such content corresponds to personalized content (e.g., of a social media network) or does not correspond to personalized content, such as premium sports-related content. In another instance, a user may be returning to a website, and accessing the website could be dependent, at least partially, on binding a user with a website and/or with an application, such as via an account for the user. In another example, a user may actuate a 'click-to-call' selector of a website and/or application to reach customer care. Thus, a third party may comprise a customer care facility of an enterprise, for example, such as a care facility of a bank, which may manage affairs related to new customer credit accounts, changes to existing credit accounts, and/or manage a host of other matters related to customer credit. Yet another scenario may involve confidentiality associated with access to medical records of patients, such as compliance with HIPAA, the Affordable Care Act, Electronic Medical Records, and/or other regulatory schemes. A variety of potential situations may arise in which a user may seek access to records, such as a patient, a company, such as for insurance, a hospital, a medical professional providing care, etc. Thus, again, a subscriber or authorized agent may log into a subscriber's medical record account that may exist online and/or be stored electronically, such as on a website. In particular scenarios, medical records access may be granted in response to a subscriber completing an application in which proper credentials are to be supplied. As yet another example, a variety of corporate programs, including as examples, airline mileage accounts, gift cards, etc., in which value has been accumulated, may be managed as online accounts, which may be accessed in response to a subscriber completing an application for such access. Thus, all of the foregoing examples, and others, accounts are subject to risk associated with fraud and/or unauthorized actions by an unscrupulous individual.

Thus, in possible scenarios, an unscrupulous individual may attempt, for example, to fraudulently obtain credit, for example, utilizing a communications device belonging to a different subscriber. However, by accessing a data store, a financial institution, for example, may challenge credentials of the unscrupulous individual, such as by accessing a data store to detecting whether a transfer (e.g., a porting event) associated with the purported subscriber's account identifier has recently occurred. A data store may also provide an indication of a subscriber's communications device has undergone a replacement of a SIM, an indication of a subscriber's tenure of position of a communications device, whether a subscriber has recently reset a password (such as the receipt of a one-time password), or as engaged in any other activity related to a device that could indicate potential for fraudulent activity. Preventing fraudulent transactions may bring about a reduction in instances of identity theft, fraud related to credit cards or other instruments, circumventing of parental controls, and so on.

In the context of the present patent application, the term "connection," the term "component" and/or similar terms are intended to be physical, but are not necessarily always tangible. Whether or not these terms refer to tangible subject

26

matter, thus, may vary in a particular context of usage. As an example, a tangible connection and/or tangible connection path may be made, such as by a tangible, electrical connection, such as an electrically conductive path comprising metal or other conductor, that is able to conduct electrical current between two tangible components. Likewise, a tangible connection path may be at least partially affected and/or controlled, such that, as is typical, a tangible connection path may be open or closed, at times resulting from influence of one or more externally derived signals, such as external currents and/or voltages, such as for an electrical switch. Non-limiting illustrations of an electrical switch include a transistor, a diode, etc. However, a "connection" and/or "component," in a particular context of usage, likewise, although physical, can also be non-tangible, such as a connection between a client and a server over a network, particularly a wireless network, which generally refers to the ability for the client and server to transmit, receive, and/or exchange communications, as discussed in more detail later.

In a particular context of usage, such as a particular context in which tangible components are being discussed, therefore, the terms "coupled" and "connected" are used in a manner so that the terms are not synonymous. Similar terms may also be used in a manner in which a similar intention is exhibited. Thus, "connected" is used to indicate that two or more tangible components and/or the like, for example, are tangibly in direct physical contact. Thus, using the previous example, two tangible components that are electrically connected are physically connected via a tangible electrical connection, as previously discussed. However, "coupled," is used to mean that potentially two or more tangible components are tangibly in direct physical contact. Nonetheless, "coupled" is also used to mean that two or more tangible components and/or the like are not necessarily tangibly in direct physical contact, but are able to co-operate, liaise, and/or interact, such as, for example, by being "optically coupled." Likewise, the term "coupled" is also understood to mean indirectly connected. It is further noted, in the context of the present patent application, since memory, such as a memory component and/or memory states, is intended to be non-transitory, the term physical, at least if used in relation to memory necessarily implies that such memory components and/or memory states, continuing with the example, are tangible.

Additionally, in the present patent application, in a particular context of usage, such as a situation in which tangible components (and/or similarly, tangible materials) are being discussed, a distinction exists between being "on" and being "over." As an example, deposition of a substance "on" a substrate refers to a deposition involving direct physical and tangible contact without an intermediary, such as an intermediary substance, between the substance deposited and the substrate in this latter example; nonetheless, deposition "over" a substrate, while understood to potentially include deposition "on" a substrate (since being "on" may also accurately be described as being "over"), is understood to include a situation in which one or more intermediaries, such as one or more intermediary substances, are present between the substance deposited and the substrate so that the substance deposited is not necessarily in direct physical and tangible contact with the substrate.

A similar distinction is made in an appropriate particular context of usage, such as in which tangible materials and/or tangible components are discussed, between being "beneath" and being "under." While "beneath," in such a particular context of usage, is intended to necessarily imply physical and tangible contact (similar to "on," as just

US 12,200,816 B2

27

described), “under” potentially includes a situation in which there is direct physical and tangible contact, but does not necessarily imply direct physical and tangible contact, such as if one or more intermediaries, such as one or more intermediary substances, are present. Thus, “on” is understood to mean “immediately over” and “beneath” is understood to mean “immediately under.”

It is likewise appreciated that terms such as “over” and “under” are understood in a similar manner as the terms “up,” “down,” “top,” “bottom,” and so on, previously mentioned. These terms may be used to facilitate discussion, but are not intended to necessarily restrict scope of claimed subject matter. For example, the term “over,” as an example, is not meant to suggest that claim scope is limited to only situations in which an embodiment is right side up, such as in comparison with the embodiment being upside down, for example. An example includes a flip chip, as one illustration, in which, for example, orientation at various times (e.g., during fabrication) may not necessarily correspond to orientation of a final product. Thus, if an object, as an example, is within applicable claim scope in a particular orientation, such as upside down, as one example, likewise, it is intended that the latter also be interpreted to be included within applicable claim scope in another orientation, such as right side up, again, as an example, and vice-versa, even if applicable literal claim language has the potential to be interpreted otherwise. Of course, again, as always has been the case in the specification of a patent application, particular context of description and/or usage provides helpful guidance regarding reasonable inferences to be drawn.

Unless otherwise indicated, in the context of the present patent application, the term “or” if used to associate a list, such as A, B, or C, is intended to mean A, B, and C, here used in the inclusive sense, as well as A, B, or C, here used in the exclusive sense. With this understanding, “and” is used in the inclusive sense and intended to mean A, B, and C; whereas “and/or” can be used in an abundance of caution to make clear that all of the foregoing meanings are intended, although such usage is not required. In addition, the term “one or more” and/or similar terms is used to describe any feature, structure, characteristic, and/or the like in the singular, “and/or” is also used to describe a plurality and/or some other combination of features, structures, characteristics, and/or the like. Likewise, the term “based on” and/or similar terms are understood as not necessarily intending to convey an exhaustive list of factors, but to allow for existence of additional factors not necessarily expressly described.

Furthermore, it is intended, for a situation that relates to implementation of claimed subject matter and is subject to testing, measurement, and/or specification regarding degree, that the particular situation be understood in the following manner. As an example, in a given situation, assume a value of a physical property is to be measured. If alternatively reasonable approaches to testing, measurement, and/or specification regarding degree, at least with respect to the property, continuing with the example, is reasonably likely to occur to one of ordinary skill, at least for implementation purposes, claimed subject matter is intended to cover those alternatively reasonable approaches unless otherwise expressly indicated. As an example, if a plot of measurements over a region is produced and implementation of claimed subject matter refers to employing a measurement of slope over the region, but a variety of reasonable and alternative techniques to estimate the slope over that region

28

exist, claimed subject matter is intended to cover those reasonable alternative techniques unless otherwise expressly indicated.

To the extent claimed subject matter is related to one or more particular measurements, such as with regard to physical manifestations capable of being measured physically, such as, without limit, temperature, pressure, voltage, current, electromagnetic radiation, etc., it is believed that claimed subject matter does not fall with the abstract idea of judicial exception to statutory subject matter. Rather, it is asserted, that physical measurements are not mental steps and, likewise, are not abstract ideas.

It is noted, nonetheless, that a typical measurement model employed is that one or more measurements may respectively comprise a sum of at least two components. Thus, for a given measurement, for example, one component may comprise a deterministic component, which in an ideal sense, may comprise a physical value (e.g., sought via one or more measurements), often in the form of one or more signals, signal samples and/or states, and one component may comprise a random component, which may have a variety of sources that may be challenging to quantify. At times, for example, lack of measurement precision may affect a given measurement. Thus, for claimed subject matter, a statistical or stochastic model may be used in addition to a deterministic model as an approach to identification and/or prediction regarding one or more measurement values that may relate to claimed subject matter.

For example, a relatively large number of measurements may be collected to better estimate a deterministic component. Likewise, if measurements vary, which may typically occur, it may be that some portion of a variance may be explained as a deterministic component, while some portion of a variance may be explained as a random component. Typically, it is desirable to have stochastic variance associated with measurements be relatively small, if feasible. That is, typically, it may be preferable to be able to account for a reasonable portion of measurement variation in a deterministic manner, rather than a stochastic matter as an aid to identification and/or predictability.

Along these lines, a variety of techniques have come into use so that one or more measurements may be processed to better estimate an underlying deterministic component, as well as to estimate potentially random components. These techniques, of course, may vary with details surrounding a given situation. Typically, however, more complex problems may involve use of more complex techniques. In this regard, as alluded to above, one or more measurements of physical manifestations may be modeled deterministically and/or stochastically. Employing a model permits collected measurements to potentially be identified and/or processed, and/or potentially permits estimation and/or prediction of an underlying deterministic component, for example, with respect to later measurements to be taken. A given estimate may not be a perfect estimate; however, in general, it is expected that on average one or more estimates may better reflect an underlying deterministic component, for example, if random components that may be included in one or more obtained measurements, are considered. Practically speaking, of course, it is desirable to be able to generate, such as through estimation approaches, a physically meaningful model of processes affecting measurements to be taken.

In some situations, however, as indicated, potential influences may be complex. Therefore, seeking to understand appropriate factors to consider may be particularly challenging. In such situations, it is, therefore, not unusual to employ heuristics with respect to generating one or more estimates.

US 12,200,816 B2

29

Heuristics refers to use of experience related approaches that may reflect realized processes and/or realized results, such as with respect to use of historical measurements, for example. Heuristics, for example, may be employed in situations where more analytical approaches may be overly complex and/or nearly intractable. Thus, regarding claimed subject matter, an innovative feature may include, in an example embodiment, heuristics that may be employed, for example, to estimate and/or predict one or more measurements.

It is further noted that the terms “type” and/or “like,” if used, such as with a feature, structure, characteristic, and/or the like, using “optical” or “electrical” as simple examples, means at least partially of and/or relating to the feature, structure, characteristic, and/or the like in such a way that presence of minor variations, even variations that might otherwise not be considered fully consistent with the feature, structure, characteristic, and/or the like, do not in general prevent the feature, structure, characteristic, and/or the like from being of a “type” and/or being “like,” (such as being an “optical-type” or being “optical-like,” for example) if the minor variations are sufficiently minor so that the feature, structure, characteristic, and/or the like would still be considered to be substantially present with such variations also present. Thus, continuing with this example, the terms optical-type and/or optical-like properties are necessarily intended to include optical properties. Likewise, the terms electrical-type and/or electrical-like properties, as another example, are necessarily intended to include electrical properties. It should be noted that the specification of the present patent application merely provides one or more illustrative examples and claimed subject matter is intended to not be limited to one or more illustrative examples; however, again, as has always been the case with respect to the specification of a patent application, particular context of description and/or usage provides helpful guidance regarding reasonable inferences to be drawn.

With advances in technology, it has become more typical to employ distributed computing and/or communication approaches in which portions of a process, such as signal processing of signal samples, for example, may be allocated among various devices, including one or more client devices and/or one or more server devices, via a computing and/or communications network, for example. A network may comprise two or more devices, such as network devices and/or computing devices, and/or may couple devices, such as network devices and/or computing devices, so that signal communications, such as in the form of signal packets and/or signal frames (e.g., comprising one or more signal samples), for example, may be exchanged, such as between a server device and/or a client device, as well as other types of devices, including between wired and/or wireless devices coupled via a wired and/or wireless network, for example.

In the context of the present patent application, the term network device refers to any device capable of communicating via and/or as part of a network and may comprise a computing device. While network devices may be capable of communicating signals (e.g., signal packets and/or frames), such as via a wired and/or wireless network, they may also be capable of performing operations associated with a computing device, such as arithmetic and/or logic operations, processing and/or storing operations (e.g., storing signal samples), such as in memory as tangible, physical memory states, and/or may, for example, operate as a server device and/or a client device in various embodiments. Network devices capable of operating as a server device, a client device and/or otherwise, may include, as examples, dedi-

30

cated rack-mounted servers, desktop computers, laptop computers, set top boxes, tablets, netbooks, smart phones, wearable devices, integrated devices combining two or more features of the foregoing devices, and/or the like, or any combination thereof. As mentioned, signal packets and/or frames, for example, may be exchanged, such as between a server device and/or a client device, as well as other types of devices, including between wired and/or wireless devices coupled via a wired and/or wireless network, for example, or any combination thereof. It is noted that the terms, server, server device, server computing device, server computing platform and/or similar terms are used interchangeably. Similarly, the terms client, client device, client computing device, client computing platform and/or similar terms are also used interchangeably. While in some instances, for ease of description, these terms may be used in the singular, such as by referring to a “client device” or a “server device,” the description is intended to encompass one or more client devices and/or one or more server devices, as appropriate. Along similar lines, references to a “database” are understood to mean, one or more databases and/or portions thereof, as appropriate.

It should be understood that for ease of description, a network device (also referred to as a networking device) may be embodied and/or described in terms of a computing device and vice-versa. However, it should further be understood that this description should in no way be construed so that claimed subject matter is limited to one embodiment, such as only a computing device and/or only a network device, but, instead, may be embodied as a variety of devices or combinations thereof, including, for example, one or more illustrative examples.

In the context of the present patent application, the term sub-network and/or similar terms, if used, for example, with respect to a network, refers to the network and/or a part thereof. Sub-networks may also comprise links, such as physical links, connecting and/or coupling nodes, so as to be capable to communicate signal packets and/or frames between devices of particular nodes, including via wired links, wireless links, or combinations thereof. Various types of devices, such as network devices and/or computing devices, may be made available so that device interoperability is enabled and/or, in at least some instances, may be transparent. In the context of the present patent application, the term “transparent,” if used with respect to devices of a network, refers to devices communicating via the network in which the devices are able to communicate via one or more intermediate devices, such as one or more intermediate nodes, but without the communicating devices necessarily specifying the one or more intermediate nodes and/or the one or more intermediate devices of the one or more intermediate nodes and/or, thus, may include within the network the devices communicating via the one or more intermediate nodes and/or the one or more intermediate devices of the one or more intermediate nodes, but may engage in signal communications as if such intermediate nodes and/or intermediate devices are not necessarily involved. For example, a router may provide a link and/or connection between otherwise separate and/or independent LANs.

The term electronic file and/or the term electronic document are used throughout this document to refer to a set of stored memory states and/or a set of physical signals associated in a manner so as to thereby, at least logically, form a file (e.g., electronic) and/or an electronic document. That is, it is not meant to implicitly reference a particular syntax, format and/or approach used, for example, with respect to a

US 12,200,816 B2

31

set of associated memory states and/or a set of associated physical signals. If a particular type of file storage format and/or syntax, for example, is intended, it is referenced expressly. It is further noted an association of memory states, for example, may be in a logical sense and not necessarily in a tangible, physical sense. Thus, although signal and/or state components of a file and/or an electronic document, for example, are to be associated logically, storage thereof, for example, may reside in one or more different places in a tangible, physical memory, in an embodiment.

Also, for one or more embodiments, an electronic document and/or electronic file may comprise a number of components. As previously indicated, in the context of the present patent application, a component is physical, but is not necessarily tangible. As an example, components with reference to an electronic document and/or electronic file, in one or more embodiments, may comprise text, for example, in the form of physical signals and/or physical states (e.g., capable of being physically displayed). Typically, memory states, for example, comprise tangible components, whereas physical signals are not necessarily tangible, although signals may become (e.g., be made) tangible, such as if appearing on a tangible display, for example, as is common. Also, for one or more embodiments, components with reference to an electronic document and/or electronic file may comprise a graphical object, such as, for example, an image, such as a digital image, and/or sub-objects, including attributes thereof, which, again, comprise physical signals and/or physical states (e.g., capable of being tangibly displayed). In an embodiment, digital content may comprise, for example, text, images, audio, video, and/or other types of electronic documents and/or electronic files, including portions thereof, for example.

For one or more embodiments, a device, such as a computing device and/or networking device, may comprise, for example, any of a wide range of digital electronic devices, including, but not limited to, desktop and/or notebook computers, high-definition televisions, digital versatile disc (DVD) and/or other optical disc players and/or recorders, game consoles, satellite television receivers, cellular telephones, tablet devices, wearable devices, personal digital assistants, mobile audio and/or video playback and/or recording devices, Internet of Things (IoT) type devices, or any combination of the foregoing. Further, unless specifically stated otherwise, a process as described, such as with reference to flow diagrams and/or otherwise, may also be executed and/or affected, in whole or in part, by a computing device and/or a network device. A device, such as a computing device and/or network device, may vary in terms of capabilities and/or features. Claimed subject matter is intended to cover a wide range of potential variations. For example, a device may include a numeric keypad and/or other display of limited functionality, such as a monochrome liquid crystal display (LCD) for displaying text, for example. In contrast, however, as another example, a web-enabled device may include a physical and/or a virtual keyboard, mass storage, one or more accelerometers, one or more gyroscopes, global positioning system (GPS) and/or other location-identifying type capability, and/or a display with a higher degree of functionality, such as a touch-sensitive color 2D or 3D display, for example.

As suggested previously, communications between a computing device and/or a network device and a wireless network may be in accordance with known and/or to be developed network protocols including, for example, global system for mobile communications (GSM), enhanced data rate for GSM evolution (EDGE), 802.11b/g/n/h, etc., and/or

32

worldwide interoperability for microwave access (WiMAX). As suggested previously, a computing device and/or a networking device may also have a subscriber identity module (SIM) card, which, for example, may comprise a detachable or embedded smart card that is able to store subscription content of a user, and/or is also able to store a contact list. It is noted, as previously mentioned, that a SIM card may also be electronic in the sense that it may simply be sorted in a particular location in memory of the computing and/or networking device. A user may own the computing device and/or network device or may otherwise be a user, such as a primary user, for example. A device may be assigned an address by a wireless network operator, a wired network operator, and/or an Internet Service Provider (ISP). For example, an address may comprise a domestic or international telephone number, an Internet Protocol (IP) address, and/or one or more other identifiers. In other embodiments, a computing and/or communications network may be embodied as a wired network, wireless network, or any combinations thereof.

A computing and/or network device may include and/or may execute a variety of now known and/or to be developed operating systems, derivatives and/or versions thereof, including computer operating systems, such as Windows, iOS, Linux, a mobile operating system, such as iOS, Android, Windows Mobile, and/or the like. A computing device and/or network device may include and/or may execute a variety of possible applications, such as a client software application enabling communication with other devices. For example, one or more messages (e.g., content) may be communicated, such as via one or more protocols, now known and/or later to be developed, suitable for communication of email, short message service (SMS), and/or multimedia message service (MMS), including via a network, such as a social network, formed at least in part by a portion of a computing and/or communications network. A computing and/or network device may also include executable computer instructions to process and/or communicate digital content, such as, for example, textual content, digital multimedia content, and/or the like. A computing and/or network device may also include executable computer instructions to perform a variety of possible tasks, such as browsing, searching, playing various forms of digital content, including locally stored and/or streamed video, and/or games such as, but not limited to, fantasy sports leagues. The foregoing is provided merely to illustrate that claimed subject matter is intended to include a wide range of possible features and/or capabilities.

In the preceding description, various aspects of claimed subject matter have been described. For purposes of explanation, specifics, such as amounts, systems and/or configurations, as examples, were set forth. In other instances, well-known features were omitted and/or simplified so as not to obscure claimed subject matter. While certain features have been illustrated and/or described herein, many modifications, substitutions, changes and/or equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all modifications and/or changes as fall within claimed subject matter.

What is claimed is:

1. A method comprising:

electronically verifying, via a particular authentication operation at a computing device, possession of a communications device by a subscriber of a communications network at least in part by:

US 12,200,816 B2

33

receiving, from the communications device, an authentication request that includes a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation, and
determining that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window;
receiving, at the computing device via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network;
determining, at the computing device, an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII; and
communicating, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network.

2. The method of claim 1, wherein the electronically verifying possession of the communications device comprises electronically verifying possession of the communications device via one or more communications enabled by a subscriber identity module (SIM) of the communications device for the communications network.

3. The method of claim 2, wherein the one or more communications enabled by the SIM of the communications device comprise at least one of the following:

- a Short Messaging Service (SMS) communication over the communications network;
- a communication between the communications device and a communication services carrier over the communications network; or
- any combination thereof.

4. The method of claim 3, wherein the SMS communication over the communications network comprises a one-time passcode (OTP).

5. The method of claim 3, wherein the communication between the communications device and the communication services carrier comprises one or more secure communications to establish a communication channel between the communications device and the communication services carrier.

6. The method of claim 5, wherein the one or more secure communications is implemented at least in part via at least one of the following: a Secure User Plane Location (SUPL) Location Platform (SLP); a SUPL Location Center (SLC); a SUPL Positioning Center (SPC); a Position Determining Entity (PDE); a gateway mobile location center (GMLC); an Enhanced Serving Mobile Location Center (E-SMLC); or any combination thereof.

7. The method of claim 2, wherein the SIM of the communications device comprises a detachable SIM card or an embedded SIM (eSIM) card.

8. The method of claim 1, wherein the received at least the portion of the PII is provided by the subscriber of the communications network via a user interface of the communications device.

34

9. The method of claim 1, wherein the determining the identity of the subscriber of the communications network comprises determining the identity from multiple identities of subscribers that have been associated with the communications device.

10. The method of claim 1, wherein the complement set of PII comprises a complement to the received at least the portion of the PII, and wherein the received at least the portion of the PII comprises at least one of the following with respect to the subscriber: a full social security number (SSN); a partial SSN; a full date-of-birth (DOB); a partial DOB; a full name; a partial name; a full physical address; a partial physical address; a full employer name; a partial employer name; a full identification number assigned to the subscriber; a partial identification number assigned to the subscriber; or any combination thereof.

11. The method of claim 1, wherein additional content to be pre-filled on the display of the communications device comprises at least one of: financial content; business content; personal content; personalized content; medical content; or any combination thereof.

12. The method of claim 1, wherein the communications network comprises a cellular communications network, at least in part, and wherein the communications device comprises a mobile communications device.

13. The method of claim 1, wherein the pre-filling the complement set of PII on the display of the communications device is implemented via a browser-based session.

14. The method of claim 13, wherein the browser-based session is initiated responsive to at least one of the following: capturing an image of a machine-readable layout via an imaging device accessible to the communications device; the subscriber interacting with a user interface of the communications device; or any combination thereof.

15. The method of claim 14, wherein the machine-readable layout comprises a quick response (QR) code, and wherein the user interface comprises a graphical user interface (GUI).

16. The method of claim 1, wherein the pre-filling the complement set of PII on the display of the communications device is implemented via a computer process executing on the communications device.

17. The method of claim 16, wherein the computer process is initiated responsive to capturing an image of a machine-readable layout via an imaging device accessible to the communications device, and wherein the computer process comprises a client software application.

18. An apparatus comprising:

- a communication interface to communicate with a transceiver of a communications device via a communications network; and
- at least one processor coupled to a memory and to the communication interface, the communication interface and the at least one processor to:

electronically verify, via a particular authentication operation, possession of the communications device by a subscriber of the communications network at least in part via:

- an acquisition, from the communications device, of a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation, and

35

a determination that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window;
receive, via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network;
determine an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII; and
communicate, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network.
19. The apparatus of claim 18, wherein possession of the communications device by the subscriber of the communications network is electronically verified via one or more communications enabled by a subscriber identity module (SIM) of the communications device for the communications network.
20. A non-transitory storage medium having instructions executable by a special-purpose computing platform to:
electronically verify, via a particular authentication operation, possession of a communications device by a subscriber of a communications network at least in part via;

36

an acquisition, from the communications device, of a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation, and
a determination that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window;
receive, via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network;
determine an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII; and
communicate, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network.

* * * * *

EXHIBIT C

Exhibit C**KYXStart's Infringement of U.S. Patent No. 12,058,528 ("528 Patent")**

Exemplary Claim	Exemplary Features in Accused Products
[1pre] A method comprising:	To the extent the preamble is limiting, the Accused Products include a method performed by an identity verifier computing device. For example, KYXStart operates a cloud-based identity verification platform accessible through a unified API that performs verification methods in real time. KYXStart's platform, including its Trusted Autofill, Telco Intelligence, Person Verification, and Fraud Intelligence products, practices a verification method using an identity verifier computing device. The KYX API is a unified programmatic interface that orchestrates identity verification steps, including device possession verification, PII reception, identity determination, and pre-filling of identity data. "The KYX API delivers streamlined, scalable integration through a single token and endpoint, giving organizations access to premium verification services fine-tuned for regions across the globe." Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) "We built a unified platform that orchestrates thousands of data sources to verify identities in milliseconds, not days." Source: https://web.archive.org/web/20260921144605/https://www.kyxstart.com/company "Modular solutions designed to scale. Activate only what you need, when you need it, through a single unified API." Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) "KYXStart provides one developer friendly API to run real time identity verification across countries and customer types."

Exemplary Claim	Exemplary Features in Accused Products
[1a] receiving, by an identity verifier computing device from a communications device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity;	Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification The Accused Products receive, by an identity verifier computing device from a communications device, a signal to verify a subscriber is co-located with a communications device, wherein the subscriber has a real-world identity. For example, KYXStart’s platform receives a request to verify identity of a subscriber co-locating with and using a communications device, such as a smartphone. KYXStart’s platform further performs real-time, electronic verification of phone number possession using carrier-grade data—i.e., data originating from the communications network. Furthermore, KYXStart’s platform further confirms the subscriber has a real-world identity by validating identity attributes such as name, date of birth, address, and phone linkage. “Leverage carrier data to verify phone number possession, check for SIM swaps, and validate user location history.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) “Carrier-grade phone intelligence: possession, SIM-swap, tenure, line type.” Source: https://www.kyxstart.ai/ (product page) “Use Telco Intelligence to validate phone possession and detect risky changes.” Source: https://web.archive.org/web/20260921144935/https://www.kyxstart.com/fintech

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that, on the left, user submits personal information to KYXStart’s platform for verification in the form of a verification request, shown on the right) “Score risk during signup, login, password reset, and payout setup · Detect suspicious devices and abnormal behavior in real time · Identify SIM swap and number porting risk before account takeover” Source: https://web.archive.org/web/20260921144935/https://www.kyxstart.com/fintech “Phone intelligence reads risk indicators tied to a number in real time—line type, activation age, reachability, SIM swap, and number portability.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “KYXStart Person Verification is built for modern onboarding flows where speed matters and accuracy cannot slip. Our identity engine verifies key attributes using trusted sources and returns a clear match result with a confidence score. You can validate identity details such as name, date of birth, address, and phone linkage in seconds.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “KYXStart helps you confirm real identity in real time using authoritative identity data and intelligent sequencing.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “2) Replace ‘SMS-only’ with adaptive authentication · Prefer passkeys, app-based push, or FIDO2 for everyday authentication. · When SMS must be used (e.g., regulatory constraints, legacy systems), pair it with real-time number intelligence: recent SIM swap status, call-forwarding detection, number recycling, active/inactive state, and port-out activity within a cooling-off window. If signals look risky, step up to face-to-face verification or alternative factors.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover “Best practices that keep results strong ... Decouple checks from SMS OTP. SMS is useful, yet fragile. If a SIM swap pops, avoid sending codes to a compromised channel.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “How can phone intelligence help identify risks early?

Exemplary Claim	Exemplary Features in Accused Products
	Phone intelligence reads risk indicators tied to a number in real time—line type, activation age, reachability, SIM swap, and number portability. Those signals surface potential fraud before funds move or credentials change. Teams can then step up authentication, hold a transaction, or route to review. The result is early detection without carpet-bombing good users with friction.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “What role does mobile identity play in fraud prevention? A mobile identity signal bridges the gap between a claimed person and their mobile number. Stability over time, activity on a legitimate mobile network, and consistent country data all support trust. When those signals wobble—fresh activation, VoIP where a mobile number is expected—you have cause to look closer. That’s how you stop identity theft and account takeover with less friction.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “What we are helping with our customers is in the entire digital life cycle. So from onboarding, to doing a strong KYC or KYB, in case of business entities, to verifying is this really their payments. And we go one step further. We also verify, ‘Is this your email address or is this your phone number?’ And to take that thing one step further, we are connected to global telco network providers, but we also do proof of possession that when you get an one-time passcode or when you use our technology, which is silent mobile auth, we can also verify you're holding the phone as well. And we've done that globally.” Source: https://www.youtube.com/watch?v=ePH2g7viHwk at 11:37-12:19
[1b] establishing, by the identity verifier computing device, a plurality of nodes of an identity network, wherein:	The Accused Products establish a plurality of nodes of an identity network, wherein the network exists in an electronic or digital domain. For example, KYXStart’s platform is designed to “[c]ombine identity, payment, phone, fraud, and risk signals into one decision engine.” Further, KYXStart’s platform establishes an identity network for each subscriber, where the network has multiple nodes tracking various aspects of the subscriber,

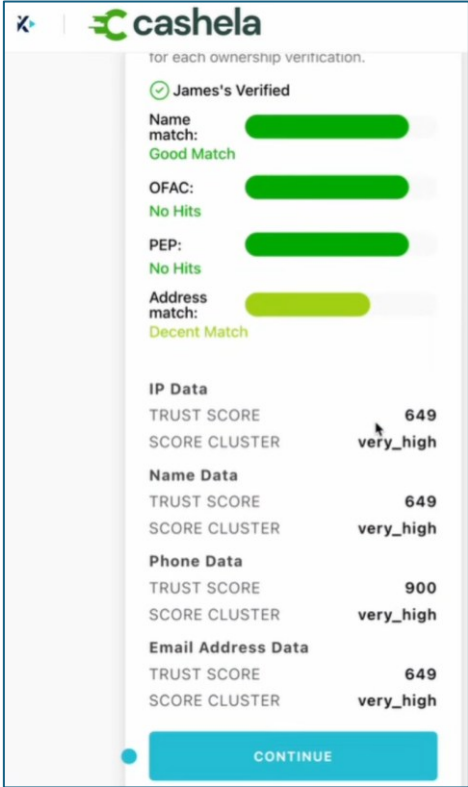
Exemplary Claim	Exemplary Features in Accused Products
the identity network exists in an electronic or digital domain,	such as name, address, phone, email address, fraud risks, etc. As KYXStart’s platform operates in the digital domain, the identify network exists in a digital domain. “Combine identity, payment, phone, fraud, and risk signals into one decision engine instead of relying on fragmented point solutions.” <i>Source:</i> https://www.kyxstart.ai/ “3) Add location intelligence that resists spoofing · Build a trusted-location graph for each customer—home, work, regular touchpoints. A request from a new place isn’t bad on its own; a request from a place that contradicts device telemetry or shows spoofing traces deserves friction. Illustratively, vendors show how tamper detection catches GPS spoofing and emulators that would otherwise pollute location signals.” <i>Source:</i> https://web.archive.org/web/20260921145014/https://www.kyxstart.com/blog/deepfake-defense-futureproof-your-identity-verification

Exemplary Claim	Exemplary Features in Accused Products
	 for each ownership verification. ✓ James's Verified Name match: ██████████ Good Match OFAC: ██████████ No Hits PEP: ██████████ No Hits Address match: ██████████ Decent Match IP Data TRUST SCORE 649 SCORE CLUSTER very_high Name Data TRUST SCORE 649 SCORE CLUSTER very_high Phone Data TRUST SCORE 900 SCORE CLUSTER very_high Email Address Data TRUST SCORE 649 SCORE CLUSTER very_high CONTINUE Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that KYXStart's platform includes an identity network for tracking subscriber James Smith) “Embrace new markets with modular identity and business verification. Open the door to more than 5 billion consumers in 195 countries. One platform, one API and one integration unlock access to 450 data sources in 43 languages.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/

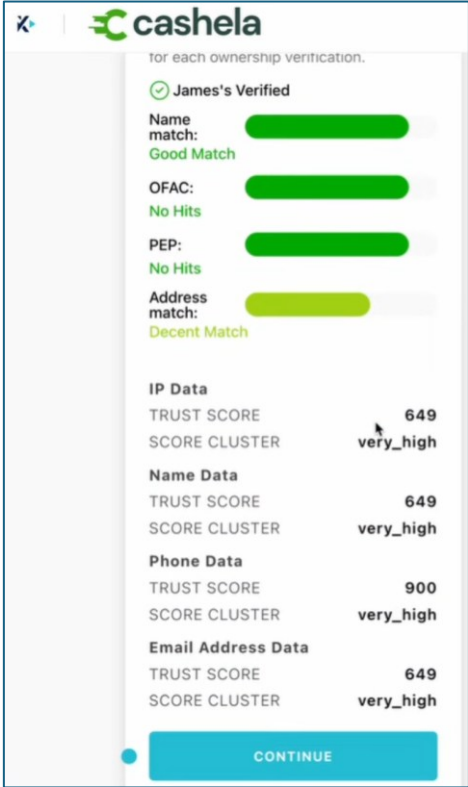
Exemplary Claim	Exemplary Features in Accused Products
	“We built a unified platform that orchestrates thousands of data sources to verify identities in milliseconds, not days.” Source: https://web.archive.org/web/20260921144605/https://www.kyxstart.com/company “Keep it alive. ... That backdrop argues for dynamic KYC refresh keyed to risk triggers—name/address changes, abnormal device churn, or a shift in the user’s payment network graph.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Identity has become more and more contextual. And the more you think about it, it's in a digital journey. If you think about somebody's digital journey, right? When you are trying to market them, it's the same person. When you're trying to onboard them, it's the same person. When you're trying to let them experience your platform like make payments or move money or actually buy new stock ... Anyways, it's in my opinion, it has changed from a static way of looking at or just in point of time to a different signals that you can connect to identity. At KYXStart, I like to say that <u>we are in the business of creating an identity fabric</u> and not an identity verification.” Source: https://www.youtube.com/watch?v=nnjInlqn2Uk at 8:55-9:46 (emphasis added) “Your phone number is global, your social profile is global, and if you talk about your banking profile, that's also global. And those are the main networks that are globally connected, not your driver license, it’s not globally connected, right? Because your driver license will not work in India but your phone will work in India and UK, everywhere else, right? Your bank account will work in, let's just say, if you go to Singapore and you wanna spend, so it'll work in Singapore. So if you think about it, <u>all those signals combined actually creates today's single identity fabric</u>. And that's what I believe we are headed towards and that's what I believe that you're going to see.” Source: https://www.youtube.com/watch?v=nnjInlqn2Uk at 12:22-13:06 (emphasis added)
[1c] the identity network is associated with the real-world identity via a persistent identifier,	The Accused Products establish a plurality of nodes of an identity network, wherein the network is associated with the real-world identity via a persistent identifier.

Exemplary Claim	Exemplary Features in Accused Products
	For example, KYXStart’s platform includes, for each subscriber, an identity network that uses a persistent identifier to tie phone number(s) to a real-world identity. “We built a unified platform that orchestrates thousands of data sources to verify identities in milliseconds, not days.” Source: https://web.archive.org/web/20260921144605/https://www.kyxstart.com/company “Persistent identifiers (e.g., subscriber data elements) and prefill can reduce keying errors and spot inconsistencies early—say, a phone number that can’t be tied to the asserted identity or a device with a thin history trying to open high-limit accounts.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “You need an evolving picture of who the customer is, what devices and phone numbers they use, and how those signals change over time.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Identity has become more and more contextual. And the more you think about it, it's in a digital journey. If you think about somebody's digital journey, right? When you are trying to market them, it's the same person. When you're trying to onboard them, it's the same person. When you're trying to let them experience your platform like make payments or move money or actually buy new stock ... Anyways, it's in my opinion, it has changed from a static way of looking at or just in point of time to a different signals that you can connect to identity. At KYXStart, I like to say that <u>we are in the business of creating an identity fabric and not an identity verification.</u>” Source: https://www.youtube.com/watch?v=nnjInlqn2Uk at 8:55-9:46 (emphasis added) “Your phone number is global, your social profile is global, and if you talk about your banking profile, that's also global. And those are the main networks that are globally connected, not your driver license, it’s not globally connected, right? Because your driver license will not work in India but your phone will work in India and UK, everywhere else, right? Your bank account will

Exemplary Claim	Exemplary Features in Accused Products
	work in, let's just say, if you go to Singapore and you wanna spend, so it'll work in Singapore. So if you think about it, <u>all those signals combined actually creates today's single identity fabric</u>. And that's what I believe we are headed towards and that's what I believe that you're going to see.” Source: https://www.youtube.com/watch?v=nnjInlqn2Uk at 12:22-13:06 (emphasis added)
[1d] each node in the plurality of nodes is associated with the persistent identifier via a set of links, and	The Accused Products establish a plurality of nodes of an identity network, wherein each node in the plurality of nodes is associated with the persistent identifier via a set of links. For example, KYXStart’s platform validates identity details, such as name, address, phone data, etc., associated with a subscriber. KYXStart’s platform associates these details with the persistent identifier of the subscriber via a set of links.

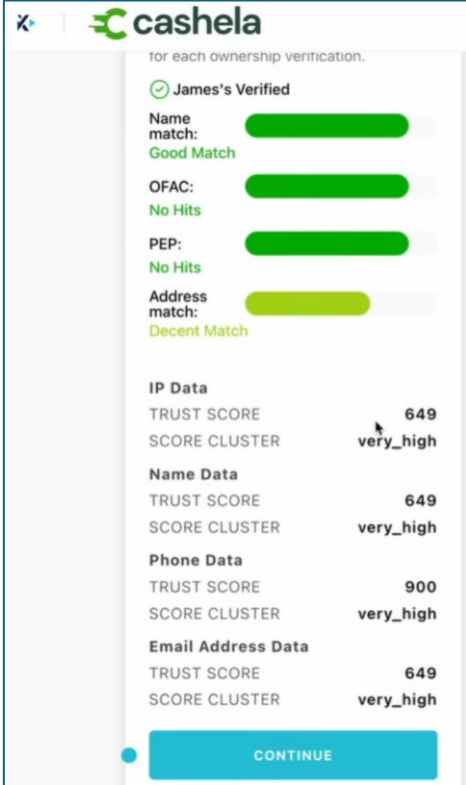
Exemplary Claim	Exemplary Features in Accused Products
	The screenshot shows the Cashela verification interface. At the top, it says "for each ownership verification." Below that, a green checkmark indicates "James's Verified". There are four rows of verification results, each with a green progress bar: "Name match: Good Match", "OFAC: No Hits", "PEP: No Hits", and "Address match: Decent Match". Below these are four sections of data: "IP Data", "Name Data", "Phone Data", and "Email Address Data". Each section has a "TRUST SCORE" of 649 and a "SCORE CLUSTER" of "very_high". At the bottom is a blue "CONTINUE" button. Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that KYXStart’s platform associates various identity details when tracking subscriber James Smith) “You can validate identity details such as name, date of birth, address, and phone linkage in seconds.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification

Exemplary Claim	Exemplary Features in Accused Products
	“Phone number intelligence layers on risk assessment: tenure, which can impact the assessment of identity risk, risk signals from the mobile network, change history, velocity across your system, and connections to identity intelligence networks.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “Keep it alive. ... That backdrop argues for dynamic KYC refresh keyed to risk triggers—name/address changes, abnormal device churn, or a shift in the user’s payment network graph.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk
[1e] each link in the set of links includes a trustworthiness parameter;	The Accused Products establish a plurality of nodes of an identity network, wherein each node in the plurality of nodes is associated with the persistent identifier via a set of links. For example, KYXStart’s platform returns “confidence scores,” “risk scores,” and composite “identity assurance” scores, which are trustworthiness parameters. Furthermore, on information and belief, each link within the identity network includes a respective trustworthiness parameter.

Exemplary Claim	Exemplary Features in Accused Products
	The screenshot shows the Cashela verification interface. At the top, it says "for each ownership verification." Below that, a green checkmark icon is followed by "James's Verified". There are four rows of verification data, each with a label, a value, and a progress bar: "Name match:" with "Good Match" and a full green bar; "OFAC:" with "No Hits" and a full green bar; "PEP:" with "No Hits" and a full green bar; and "Address match:" with "Decent Match" and a partially filled green bar. Below these are four sections of data: "IP Data", "Name Data", "Phone Data", and "Email Address Data". Each section has "TRUST SCORE" and "SCORE CLUSTER" values. For IP, Name, and Email Address, the Trust Score is 649 and the Score Cluster is "very_high". For Phone, the Trust Score is 900 and the Score Cluster is "very_high". At the bottom is a blue "CONTINUE" button. Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that KYXStart’s platform includes “TRUST SCORE” parameters into the linked details of subscriber James Smith) “Our identity engine verifies key attributes using trusted sources and returns a clear match result with a confidence score.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “Real-time risk scoring based on device fingerprinting, behavioral biometrics, and global fraud network databases.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ “Query an intelligence API for tenure, risk signals, and telecom events. Return a risk score with reasons and wire it into your rules: approve, challenge, review, or decline.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “Treat identity assurance as a composite score that blends document checks with signals like device lineage, digital footprint, telecom corroboration, and behavioral biometrics.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards “Identity Confidence Score coverage: percent of customers with multi-source corroboration at onboarding and at each high-risk event.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards
[1f] responsive to a first set of interactions by a first aspect of a set of aspects with at least a first node of the plurality of nodes, updating, by the identity verifier computing device, a first trustworthiness parameter of a first link between a second node of the plurality of nodes and a second aspect of the set of aspects; and	The Accused Products, responsive to a first set of interactions by a first aspect of a set of aspects with at least a first node of the plurality of nodes, update a first trustworthiness parameter of a first link between a second node of the plurality of nodes and a second aspect of the set of aspects. For example, KYXStart’s platform dynamically updates risk assessments and confidence scores in response to subscriber interactions and deterministic events. KYXStart advocates “dynamic KYC refresh keyed to risk triggers” including “name/address changes, abnormal device churn, or a shift in the user’s payment network graph.” The platform scores risk at each interaction event—“signup, login, password reset, and payout setup”—and feeds telco signals such as “SIM-change, port-out, call-forwarding, and line-status into [the] authentication engine.” KYXStart further recommends refreshing “KYC risk when contact data changes, devices rotate, payees shift, or spend patterns leap,” indicating that, within KYXStart’s platform, interactions at one node would trigger update to trustworthiness assessments at other nodes.

Exemplary Claim	Exemplary Features in Accused Products
	“Keep it alive. ... That backdrop argues for dynamic KYC refresh keyed to risk triggers—name/address changes, abnormal device churn, or a shift in the user’s payment network graph.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Score risk during signup, login, password reset, and payout setup · Detect suspicious devices and abnormal behavior in real time · Identify SIM swap and number porting risk before account takeover.” Source: https://web.archive.org/web/20260921144935/https://www.kyxstart.com/fintech “Refresh KYC risk when contact data changes, devices rotate, payees shift, or spend patterns leap.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards “Feed SIM-change, port-out, call-forwarding, and line-status into your authentication engine.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover “If you embed number intelligence, modern authentication, and event-based re-verification into your stack—and rehearse the operational moves that go with them—you will cut through the SIM-swap fog and make takeover far harder to pull off.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover “Treat identity as living data. Step up when risk changes: device swap, SIM swap, velocity spikes, new payee, or login from a suspicious network. Don’t wait for a calendar refresh.” Source: https://web.archive.org/web/20260921145014/https://www.kyxstart.com/blog/deepfake-defense-futureproof-your-identity-verification

Exemplary Claim	Exemplary Features in Accused Products
	 Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that KYXStart's platform dynamically keeps track of trustworthiness parameters of subscriber James Smith)
[1g] transmitting, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device,	The Accused Products transmit, by the identity verifier computing device to the communications device, a verification that the subscriber is co-located with the communications device, wherein the verification is based, at least in part, on the first link.

Exemplary Claim	Exemplary Features in Accused Products
wherein the verification is based, at least in part, on the first link.	For example, after a subscriber is verified, KYXStart’s platform transmits the verification output based on the platform’s trust assessment, which incorporates the trustworthiness parameters of the identity network links. “We needed an identity verification partner who could operate across borders without slowing down our onboarding funnel. KYXStart gave us a single API that handles document verification, liveness checks, and risk decisioning in real time, and our approval rates improved within the first month of integration.” Source: https://www.kyxstart.ai/ (customer testimonial) “Our identity engine verifies key attributes using trusted sources and returns a clear match result with a confidence score.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “Compliance used to be our bottleneck. Now it’s a competitive advantage. The realtime webhooks are lifesavers.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification (customer testimonial)

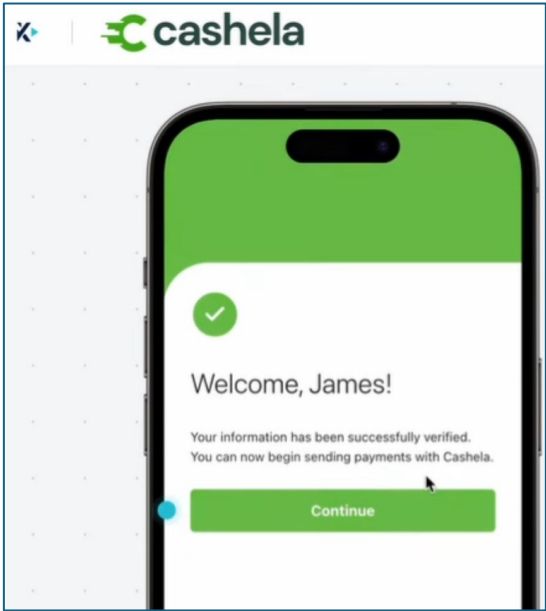
Exemplary Claim	Exemplary Features in Accused Products
	A screenshot of a mobile application interface for 'cashela'. At the top, there is a logo with a green 'C' and the word 'cashela' in black. Below the logo, a green checkmark icon is displayed above the text 'Welcome, James!'. Underneath, a smaller line of text reads: 'Your information has been successfully verified. You can now begin sending payments with Cashela.' At the bottom of the screen, there is a prominent green rectangular button with the word 'Continue' in white text. The entire interface is shown within a black smartphone frame. <i>Source: https://www.youtube.com/watch?v=meoKNa_C67A (showing that KYXStart's platform transmits a message indicating that the subscriber has been successfully verified)</i>

EXHIBIT D

Exhibit D**KYXStart's Infringement of U.S. Patent No. 12,200,816 ("816 Patent")**

Exemplary Claim	Exemplary Features in Accused Products
[1pre] A method comprising:	To the extent the preamble is limiting, the Accused Products include an electronic verification method. For example, KYXStart offers an API-based identity verification service that executes programmatic methods in real time. KYXStart's platform, including its Trusted Autofill, Telco Intelligence, Person Verification, and Fraud Intelligence products, practices an electronic verification method. The KYX API is a unified programmatic interface that orchestrates identity verification steps, including device possession verification, PII reception, identity determination, and pre-filling of identity data. “The KYX API delivers streamlined, scalable integration through a single token and endpoint, giving organizations access to premium verification services fine-tuned for regions across the globe.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) “Modular solutions designed to scale. Activate only what you need, when you need it, through a single unified API.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) “KYXStart provides one developer friendly API to run real time identity verification across countries and customer types.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “Onboarding Autofill Prefill verified identity from a phone number. Fewer fields, higher completion.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://www.kyxstart.ai/ “ ‘Financial literacy only works if the onboarding experience behind it is frictionless. KYXStart's Trusted Autofill let us cut down the steps required to get a new user started, without sacrificing the verification rigor our financial institution partners expect from us.’ Head of Partnerships, Financial Wellness and Literacy Platform” Source: https://www.kyxstart.ai/ “Accelerate onboarding with Advanced Pre-Fill KYXStart enables faster, lower-friction onboarding by helping pre-populate verified identity data from minimal user input. Our APIs are built for seamless integration, speed, and scalability, helping improve conversion and onboarding efficiency.” Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding
[1a] electronically verifying, via a particular authentication operation, possession of the communications device by a subscriber of the communications network at least in part via:	The Accused Products electronically verify, via a particular authentication operation, possession of the communications device by a subscriber of the communications network. For example, KYXStart’s Telco Intelligence product expressly verifies phone number possession by leveraging carrier data from the communications network. KYXStart’s Telco Intelligence product performs real-time, electronic verification of phone number possession using carrier-grade data—i.e., data originating from the communications network. “Leverage carrier data to verify phone number possession, check for SIM swaps, and validate user location history.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) “Carrier-grade phone intelligence: possession, SIM-swap, tenure, line type.” Source: https://www.kyxstart.ai/

Exemplary Claim	Exemplary Features in Accused Products
	“Use Telco Intelligence to validate phone possession and detect risky changes.” Source: https://web.archive.org/web/20260921144935/https://www.kyxstart.com/fintech “Phone intelligence reads risk indicators tied to a number in real time—line type, activation age, reachability, SIM swap, and number portability.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “2) Replace ‘SMS-only’ with adaptive authentication · Prefer passkeys, app-based push, or FIDO2 for everyday authentication. · When SMS must be used (e.g., regulatory constraints, legacy systems), pair it with real-time number intelligence: recent SIM swap status, call-forwarding detection, number recycling, active/inactive state, and port-out activity within a cooling-off window. If signals look risky, step up to face-to-face verification or alternative factors.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover “Best practices that keep results strong ... Decouple checks from SMS OTP. SMS is useful, yet fragile. If a SIM swap pops, avoid sending codes to a compromised channel.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “How can phone intelligence help identify risks early? Phone intelligence reads risk indicators tied to a number in real time—line type, activation age, reachability, SIM swap, and number portability. Those signals surface potential fraud before funds move or credentials change. Teams can then step up authentication, hold a transaction, or route to review. The result is early detection without carpet-bombing good users with friction.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “What role does mobile identity play in fraud prevention? A mobile identity signal bridges the gap between a claimed person and their mobile number. Stability over time, activity on a legitimate mobile network, and consistent country data all support trust. When those signals wobble—fresh activation, VoIP where a mobile number is expected—you have cause to look closer. That’s how you stop identity theft and account takeover with less friction.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “What we are helping with our customers is in the entire digital life cycle. So from onboarding, to doing a strong KYC or KYB, in case of business entities, to verifying is this really their payments. And we go one step further. We also verify, ‘Is this your email address or is this your phone number?’ And to take that thing one step further, we are connected to global telco network providers, but we also do proof of possession that when you get an one-time passcode or when you use our technology, which is silent mobile auth, we can also verify you're holding the phone as well. And we've done that globally.” Source: https://www.youtube.com/watch?v=ePH2g7viHwk at 11:37-12:19
[1b] receiving, from the communications device, an authentication request that includes a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular	The Accused Products receive, from the communications device, an authentication request that includes a time-limited-type identifier generated during the particular authentication operation, wherein the time-limited-type identifier is unique to the particular authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation. For example, KYXStart’s blog content discusses token-based authentication, hardware-backed keys, and session linkage mechanisms consistent with the use of a “time-limited-type identifier.” On information and belief, KYXStart’s platform uses session-based tracking for user authentication, where a token or identifier is generated specifically for an authentication session. Tokens or

Exemplary Claim	Exemplary Features in Accused Products
authentication operation and is passed between the computing device and the communications device so as to maintain a linkage through a plurality of steps of the particular authentication operation, and	identifiers generated for sessions are known to be time-limited-type that expire after predetermined durations. “From principles to practice: what ‘perpetual vigilance’ looks like ... Monitor · Use risk-based decisioning for every session, not just login. A clean login means little if a SIM change happened an hour before.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover “Field guide: detection signals that punch above their weight ... Device intelligence as a graph Emulators, rooted devices, headless browsers, and copy-paste autofill patterns cluster synthetics. Linking sign-ups and sessions by device prints reveals networks hiding behind clean documents.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards “Persistent device recognition across sessions and reinstalls, not just cookies and browser prints. Pair on-device biometrics with hardware-backed keys so an attacker can’t easily lift a token and replay it elsewhere.” Source: https://web.archive.org/web/20260921145014/https://www.kyxstart.com/blog/deepfake-defense-futureproof-your-identity-verification “On-device biometrics to unlock a hardware-bound key. The key signs requests, and the signature binds to device state so tokens can’t be replayed from a different environment.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://web.archive.org/web/20260921145014/https://www.kyxstart.com/blog/deepfake-defense-futureproof-your-identity-verification “Telco risk signals stitched into the auth fabric Feed SIM-change, port-out, call-forwarding, and line-status into your authentication engine. If a login + device binding looks clean but the number swapped last night, treat that session as high risk, not business as usual.” Source: https://web.archive.org/web/20260921152237/https://www.kyxstart.com/blog/sim-swap-fraud-2025-account-takeover
[1c] determining that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window;	The Accused Products determine that the time-limited-type identifier is valid based on a number of times the time-limited-type identifier has been included in one or more authentication requests received within a recent time window. For example, KYXStart’s blog content advocates velocity-based signals and session-level analysis consistent with validation of a token based on usage count within a time window. Furthermore, KYXStart’s platform performs real-time risk scoring that is based on device fingerprinting and behavioral biometrics, which would include velocity rules that track the number of times a token or identifier is reused. “Below is a practical checklist you can build into a lookup API or intelligence API. Use it to assess the risk of a phone number and return a score your teams trust. ... 6) Velocity and reuse · Signups per number, per device, per IP. · Overlap with risky clusters across millions of phone numbers. · Why it matters: mule networks recycle numbers and rotate through large application sets.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation

Exemplary Claim	Exemplary Features in Accused Products
	“A practical 90-day plan to harden your defenses Day 0–30: instrument the gaps Map your identity signals end-to-end: document, biometric, device, IP, email/phone, telecom, bureau, registry. Identify single points of failure. Stand up velocity rules on applications, device reuse, and beneficiary changes. Pilot digital-footprint checks (email/phone age, domain health, social presence) as low-friction evidence of a real person.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards “A simple framework for deepfake-resilient verification Leaders don’t need a hundred new tools. They need a playbook that makes identity expensive for attackers. Start here. ... 6) Event-driven re-verification · Treat identity as living data. Step up when risk changes: device swap, SIM swap, velocity spikes, new payee, or login from a suspicious network. Don’t wait for a calendar refresh.” Source: https://web.archive.org/web/20260921145014/https://www.kyxstart.com/blog/deepfake-defense-futureproof-your-identity-verification “Real-time risk scoring based on device fingerprinting, behavioral biometrics, and global fraud network databases.” Source: https://web.archive.org/web/20260921152306/https://www.kyxstart.com/ (homepage) “Low latency, powerful infrastructure supports very high volumes with tens of thousands of real-time calculations.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding “A number follows the customer across devices, apps, and sessions.” Source: https://web.archive.org/web/20260921144947/https://www.kyxstart.com/blog/phone-number-intelligence-fraud-risk-validation “Device and network telemetry should spot anomalies like freshly virtualized devices, high-risk ASNs, or VPNs that hop per session.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Linking sign-ups and sessions by device prints reveals networks hiding behind clean documents.” Source: https://web.archive.org/web/20260921152222/https://www.kyxstart.com/blog/synthetic-identity-fraud-the-invisible-threat-reshaping-compliance-and-kyc-standards “Design your program to check signals that models can’t magically invent—like eCBSV matches, long-lived email reputations, or device histories that persist across sessions.” Source: https://web.archive.org/web/20260921152254/https://www.kyxstart.com/blog/state-of-fraud-2025-identity-verification
[1d] receiving, at the computing device via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network;	The Accused Products receive, at the computing device via the communications network, at least a portion of personally identifiable information (PII) unique to the subscriber of the communications network. For example, KYXStart’s platform verifies a subscriber by receiving a phone number, which is a portion of personally identifiable information (PII) unique to the subscriber. KYXStart expressly describes receiving this data with “minimal user input” for purposes of identity verification. “Prefill verified identity from a phone number. Fewer fields, higher completion.”

Exemplary Claim	Exemplary Features in Accused Products
	Source: https://www.kyxstart.ai/ “You can validate identity details such as name, date of birth, address, and phone linkage in seconds.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “KYXStart helps organizations streamline digital onboarding by enabling faster identity verification with minimal user input.” Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding “KYXStart enables faster, lower-friction onboarding by helping pre-populate verified identity data from minimal user input.” Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding “When you prefill identity fields from trusted data—think telco subscriber records, government data services where available, or robust credit bureau files—you remove fat-finger risk and surface inconsistencies early.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk
[1e] determining, at the computing device, an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII; and	The Accused Products determine, at the computing device, an identity of the subscriber of the communications network based, at least in part, on the received at least the portion of the PII. For example, KYXStart’s platform determines subscriber identity by matching received PII against authoritative data sources and returning a confidence score. KYXStart’s Person Verification product receives subscriber PII (including phone number, name, date of birth, and address) and determines the subscriber’s identity by matching that PII against “thousands of data sources” using “intelligent sequencing.” The system returns “a clear match result with a confidence score,” confirming that the computing device determines an identity of the subscriber based on the received PII.

Exemplary Claim	Exemplary Features in Accused Products
	“KYXStart Person Verification is built for modern onboarding flows where speed matters and accuracy cannot slip. Our identity engine verifies key attributes using trusted sources and returns a clear match result with a confidence score.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “[We] confirm real identity in real time using authoritative identity data and intelligent sequencing.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “We built a unified platform that orchestrates thousands of data sources to verify identities in milliseconds, not days.” Source: https://web.archive.org/web/20260921144605/https://www.kyxstart.com/company “Detect mismatches, suspicious patterns, and synthetic identity risk early in the signup flow.” Source: https://web.archive.org/web/20260921144654/https://www.kyxstart.com/person-verification “Optimized data source sequencing allows for efficient verification, reducing costs while maintaining high performance.” Source: https://web.archive.org/web/20260921152307/https://www.kyxstart.com/about-us “Onboarding Autofill Prefill verified identity from a phone number. Fewer fields, higher completion.” Source: https://www.kyxstart.ai/ “ ‘Financial literacy only works if the onboarding experience behind it is frictionless. KYXStart's Trusted Autofill let us cut down the steps required to get a new user started, without sacrificing the verification rigor our financial institution partners expect from us.’ Head of Partnerships, Financial Wellness and Literacy Platform” Source: https://www.kyxstart.ai/

Exemplary Claim	Exemplary Features in Accused Products
	“Accelerate onboarding with Advanced Pre-Fill KYXStart enables faster, lower-friction onboarding by helping pre-populate verified identity data from minimal user input. Our APIs are built for seamless integration, speed, and scalability, helping improve conversion and onboarding efficiency.” Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding
[1f] communicating, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network.	The Accused Products communicate, via the communications network, a complement set of PII to be pre-filled on a display of the communications device based, at least in part, on the determined identity of the subscriber of the communications network. For example, KYXStart’s Trusted Autofill product expressly pre-fills verified identity data on the subscriber’s device based on the determined identity. KYXStart’s Trusted Autofill product communicates a complement set of PII—including verified name, address, date of birth, and other identity fields—via the communications network to be pre-filled on the display of the subscriber’s communications device. This pre-filling is expressly “based, at least in part, on the determined identity of the subscriber,” as the autofilled data is derived from the identity determination performed by KYXStart’s platform using “trusted data” including “telco subscriber records, government data services ... or robust credit bureau files.” “Prefill verified identity from a phone number. Fewer fields, higher completion.” Source: https://www.kyxstart.ai/ “ ‘Financial literacy only works if the onboarding experience behind it is frictionless. KYXStart’s Trusted Autofill let us cut down the steps required to get a new user started, without sacrificing the verification rigor our financial institution partners expect from us.’ Head of Partnerships, Financial Wellness and Literacy Platform” Source: https://www.kyxstart.ai/ (customer testimonial) “Accelerate onboarding with Advanced Pre-Fill

Exemplary Claim	Exemplary Features in Accused Products
	KYXStart enables faster, lower-friction onboarding by helping pre-populate verified identity data from minimal user input. Our APIs are built for seamless integration, speed, and scalability, helping improve conversion and onboarding efficiency.” Source: https://web.archive.org/web/20260921152335/https://www.kyxstart.com/customer-onboarding “Our onboarding flow was losing customers at the data entry stage, and our compliance team needed cleaner, more complete records to support enhanced due diligence.” Source: https://kyx-start.webflow.io/ (customer testimonial) “When you prefill identity fields from trusted data—think telco subscriber records, government data services where available, or robust credit bureau files—you remove fat-finger risk and surface inconsistencies early.” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Can we prefill a customer’s identity data from trusted sources (e.g., telco or government) to reduce manual input and catch mismatches in near real time?” Source: https://web.archive.org/web/20260921145022/https://www.kyxstart.com/blog/fbi-ic3-2024-kyc-kyb-kyp-fraud-risk “Six modular products. One contract. Switch on what you need today and activate the rest when you’re ready.” Source: https://www.kyxstart.ai/

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

PROVE IDENTITY, INC.

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Travis S. Hunter & Alexandra M. Ewing - Richards,
Layton & Finger, P.A. One Rodney Square, 920 North King
Street, Wilmington, Delaware 19801-302-651-7700

DEFENDANTS

KYXSTART, INC.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff ☒ 3 Federal Question
(U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity
(Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | | PTF | DEF | | PTF | DEF |
|---|----------------------------|----------------------------|---|----------------------------|----------------------------|
| Citizen of This State | ☐ 1 | ☐ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☐ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: [Nature of Suit Code Descriptions.](#)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 151 Medicare Act ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans) ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholders' Suits ☐ 190 Other Contract ☐ 195 Contract Product Liability ☐ 196 Franchise	PERSONAL INJURY ☐ 310 Airplane ☐ 315 Airplane Product Liability ☐ 320 Assault, Libel & Slander ☐ 330 Federal Employers' Liability ☐ 340 Marine ☐ 345 Marine Product Liability ☐ 350 Motor Vehicle ☐ 355 Motor Vehicle Product Liability ☐ 360 Other Personal Injury ☐ 362 Personal Injury - Medical Malpractice PERSONAL INJURY ☐ 365 Personal Injury - Product Liability ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability ☐ 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY ☐ 370 Other Fraud ☐ 371 Truth in Lending ☐ 380 Other Personal Property Damage ☐ 385 Property Damage Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881 ☐ 690 Other LABOR ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Management Relations ☐ 740 Railway Labor Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Employee Retirement Income Security Act IMMIGRATION ☐ 462 Naturalization Application ☐ 465 Other Immigration Actions	☐ 422 Appeal 28 USC 158 ☐ 423 Withdrawal 28 USC 157 INTELLECTUAL PROPERTY RIGHTS ☐ 820 Copyrights ☒ 830 Patent ☐ 835 Patent - Abbreviated New Drug Application ☐ 840 Trademark ☐ 880 Defend Trade Secrets Act of 2016 SOCIAL SECURITY ☐ 861 HIA (1395ff) ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) ☐ 864 SSID Title XVI ☐ 865 RSI (405(g)) FEDERAL TAX SUITS ☐ 870 Taxes (U.S. Plaintiff or Defendant) ☐ 871 IRS—Third Party 26 USC 7609	☐ 375 False Claims Act ☐ 376 Qui Tam (31 USC 3729(a)) ☐ 400 State Reapportionment ☐ 410 Antitrust ☐ 430 Banks and Banking ☐ 450 Commerce ☐ 460 Deportation ☐ 470 Racketeer Influenced and Corrupt Organizations ☐ 480 Consumer Credit (15 USC 1681 or 1692) ☐ 485 Telephone Consumer Protection Act ☐ 490 Cable/Sat TV ☐ 850 Securities/Commodities/Exchange ☐ 890 Other Statutory Actions ☐ 891 Agricultural Acts ☐ 893 Environmental Matters ☐ 895 Freedom of Information Act ☐ 896 Arbitration ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision ☐ 950 Constitutionality of State Statutes
REAL PROPERTY ☐ 210 Land Condemnation ☐ 220 Foreclosure ☐ 230 Rent Lease & Ejectment ☐ 240 Torts to Land ☐ 245 Tort Product Liability ☐ 290 All Other Real Property	CIVIL RIGHTS ☐ 440 Other Civil Rights ☐ 441 Voting ☐ 442 Employment ☐ 443 Housing/Accommodations ☐ 445 Amer. w/Disabilities - Employment ☐ 446 Amer. w/Disabilities - Other ☐ 448 Education PRISONER PETITIONS Habeas Corpus: ☐ 463 Alien Detainee ☐ 510 Motions to Vacate Sentence ☐ 530 General ☐ 535 Death Penalty Other: ☐ 540 Mandamus & Other ☐ 550 Civil Rights ☐ 555 Prison Condition ☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

35 U.S.C. § 271

Brief description of cause:
Infringement of U.S. Patents

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

Oct 14, 2026

SIGNATURE OF ATTORNEY OF RECORD

/s/ Travis S. Hunter (#5350)

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE