



(51) International Patent Classification:
H04M 3/42 (2006.01)

(21) International Application Number: PCT/US2021/056251

(22) **International Filing Date:** 22 October 2021 (22.10.2021)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) Priority Data:
17/078,652 23 October 2020 (23.10.2020) US

(71) Applicant: NUANCE COMMUNICATIONS, INC.
[US/US]: One Wayside Road, Burlington, Massachusetts
01803 (US).

(72) **Inventor:** TALIB, Haydar; 16-5360 Côte Saint-Luc Road, Montreal, Québec H3X 2C4 (CA).

(74) **Agent: SARGEANT, Heath M.** et al.; Holland & Knight LLP, 10 St. James Avenue, Boston, Massachusetts 02116 (US).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: FRAUD DETECTION SYSTEM AND METHOD

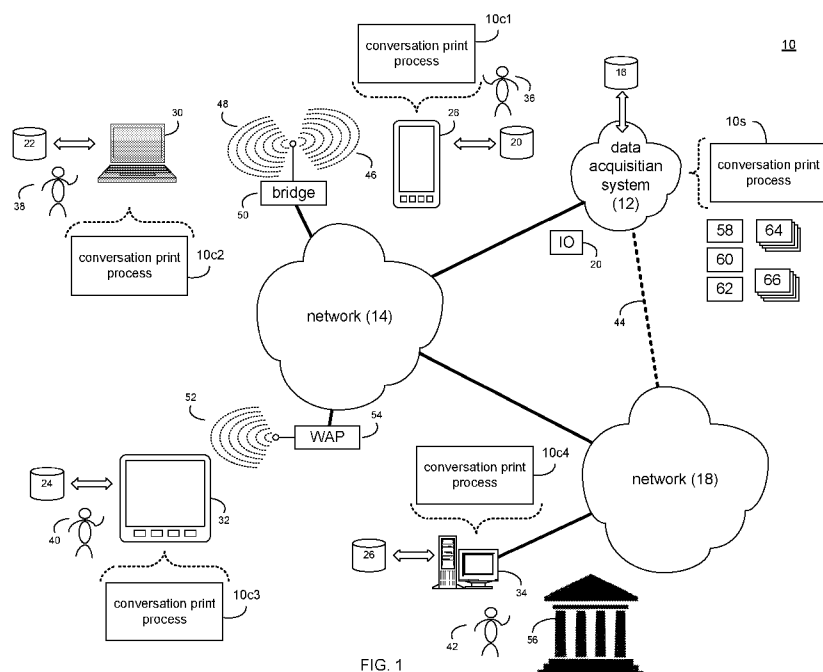


FIG. 1

(57) **Abstract:** A method, computer program product, and computing system for receiving input information concerning a conversation between a caller and a recipient; processing the input information to assess a fraud-threat-level; defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and effectuating the targeted response.

Declarations under Rule 4.17:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*

Fraud Detection System and Method

Cross-Reference to Related Application Paragraph

[001] This application claims the benefit of U.S. Non-Provisional Application No. 17/078,652, filed on October 23, 2020. The contents of which is incorporated herein in its entirety.

Technical Field

[002] This disclosure relates to conversation monitoring and, more particularly, to systems and methods that monitor conversations to detect fraudsters.

Background

[003] In many interactions between people (e.g., a customer calling a business and the customer service representative that handles the call), fraudsters often impersonate legitimate customers in an attempt to commit an act of fraud. For example, a fraudster may reach out to a credit card company and pretend to be a customer of the credit card company so that they may fraudulently obtain a copy of that customer's credit card. Unfortunately, these fraudsters are often successful, resulting in fraudulent charges, fraudulent monetary transfers, and identity theft. For obvious reasons, it is desirable to identify these fraudsters and prevent them from being successful.

Summary of Disclosure

[004] In one implementation, a computer-implemented method is executed on a computing device and includes: receiving input information concerning a conversation between a caller and a recipient; processing the input information to assess a fraud-threat-level; defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level;

and effectuating the targeted response.

[005] One or more of the following features may be included. The input information may include one or more of: a caller conversation portion; a recipient conversation portion; and biometric information concerning the caller. The conversation may include one or more of: a voice-based conversation between the caller and the recipient; and a text-based conversation between the caller and the recipient. Effectuating the targeted response may include one or more of: allowing the conversation to continue; asking a question of the caller; prompting the recipient to ask a question of the caller; effecting a transfer from the recipient to a third-party; and ending the conversation between the caller and the recipient. Processing the input information to determine a fraud-threat-level may include: determining if the input information is indicative of fraudulent behavior. Determining if the input information is indicative of fraudulent behavior may include: comparing the input information to a plurality of fraudulent behaviors. The plurality of fraudulent behaviors may include a plurality of empirically-defined fraudulent behaviors. The plurality of empirically-defined fraudulent behaviors may be defined via AI/ML processing of information concerning a plurality of earlier conversations.

[006] In another implementation, a computer program product resides on a computer readable medium and has a plurality of instructions stored on it. When executed by a processor, the instructions cause the processor to perform operations including receiving input information concerning a conversation between a caller and a recipient; processing the input information to assess a fraud-threat-level; defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and effectuating the targeted response.

[007] One or more of the following features may be included. The input information may include one or more of: a caller conversation portion; a recipient conversation portion; and biometric information concerning the caller. The conversation may include one or more of: a voice-based conversation between the caller and the recipient; and a text-based

conversation between the caller and the recipient. Effectuating the targeted response may include one or more of: allowing the conversation to continue; asking a question of the caller; prompting the recipient to ask a question of the caller; effecting a transfer from the recipient to a third-party; and ending the conversation between the caller and the recipient. Processing the input information to determine a fraud-threat-level may include: determining if the input information is indicative of fraudulent behavior. Determining if the input information is indicative of fraudulent behavior may include: comparing the input information to a plurality of fraudulent behaviors. The plurality of fraudulent behaviors may include a plurality of empirically-defined fraudulent behaviors. The plurality of empirically-defined fraudulent behaviors may be defined via AI/ML processing of information concerning a plurality of earlier conversations.

[008] In another implementation, a computing system includes a processor and memory is configured to perform operations including receiving input information concerning a conversation between a caller and a recipient; processing the input information to assess a fraud-threat-level; defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and effectuating the targeted response.

[009] One or more of the following features may be included. The input information may include one or more of: a caller conversation portion; a recipient conversation portion; and biometric information concerning the caller. The conversation may include one or more of: a voice-based conversation between the caller and the recipient; and a text-based conversation between the caller and the recipient. Effectuating the targeted response may include one or more of: allowing the conversation to continue; asking a question of the caller; prompting the recipient to ask a question of the caller; effecting a transfer from the recipient to a third-party; and ending the conversation between the caller and the recipient. Processing the input information to determine a fraud-threat-level may include: determining if the input information is indicative of fraudulent behavior. Determining if

the input information is indicative of fraudulent behavior may include: comparing the input information to a plurality of fraudulent behaviors. The plurality of fraudulent behaviors may include a plurality of empirically-defined fraudulent behaviors. The plurality of empirically-defined fraudulent behaviors may be defined via AI/ML processing of information concerning a plurality of earlier conversations.

[0010] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will become apparent from the description, the drawings, and the claims.

Brief Description of the Drawings

[0011] FIG. 1 is a diagrammatic view of a data acquisition system and a fraud detection process coupled to a distributed computing network;

[0012] FIG. 2 is a flow chart of an implementation of the fraud detection process of FIG. 1;

[0013] FIG. 3 is a diagrammatic view of a conversation transcript; and

[0014] FIG. 4 is a diagrammatic view of a plurality of fraudulent behaviors.

[0015] Like reference symbols in the various drawings indicate like elements.

Detailed Description of the Preferred Embodiments

System Overview:

[0016] Referring to FIG. 1, there is shown fraud detection process 10. As will be discussed below in greater detail, fraud detection process 10 may be configured to interface with data acquisition system 12 and detect and/or frustrate fraudsters.

[0017] Fraud detection process 10 may be implemented as a server-side process, a client-side process, or a hybrid server-side / client-side process. For example, fraud detection process 10 may be implemented as a purely server-side process via fraud

detection process 10s. Alternatively, fraud detection process 10 may be implemented as a purely client-side process via one or more of fraud detection process 10c1, fraud detection process 10c2, fraud detection process 10c3, and fraud detection process 10c4. Alternatively still, fraud detection process 10 may be implemented as a hybrid server-side / client-side process via fraud detection process 10s in combination with one or more of fraud detection process 10c1, fraud detection process 10c2, fraud detection process 10c3, and fraud detection process 10c4.

[0018] Accordingly, fraud detection process 10 as used in this disclosure may include any combination of fraud detection process 10s, fraud detection process 10c1, fraud detection process 10c2, fraud detection process 10c3, and fraud detection process 10c4.

[0019] Fraud detection process 10s may be a server application and may reside on and may be executed by data acquisition system 12, which may be connected to network 14 (e.g., the Internet or a local area network). Data acquisition system 12 may include various components, examples of which may include but are not limited to: a personal computer, a server computer, a series of server computers, a mini computer, a mainframe computer, one or more Network Attached Storage (NAS) systems, one or more Storage Area Network (SAN) systems, one or more Platform as a Service (PaaS) systems, one or more Infrastructure as a Service (IaaS) systems, one or more Software as a Service (SaaS) systems, one or more software applications, one or more software platforms, a cloud-based computational system, and a cloud-based storage platform.

[0020] As is known in the art, a SAN may include one or more of a personal computer, a server computer, a series of server computers, a mini computer, a mainframe computer, a RAID device and a NAS system. The various components of data acquisition system 12 may execute one or more operating systems, examples of which may include but are not limited to: Microsoft Windows Server [™], Redhat Linux [™], Unix, or a custom operating system, for example.

[0021] The instruction sets and subroutines of fraud detection process 10s, which may be stored on storage device 16 coupled to data acquisition system 12, may be executed by one or more processors (not shown) and one or more memory architectures (not shown) included within data acquisition system 12. Examples of storage device 16 may include but are not limited to: a hard disk drive; a RAID device; a random access memory (RAM); a read-only memory (ROM); and all forms of flash memory storage devices.

[0022] Network 14 may be connected to one or more secondary networks (e.g., network 18), examples of which may include but are not limited to: a local area network; a wide area network; or an intranet, for example.

[0023] Various IO requests (e.g. IO request 20) may be sent from fraud detection process 10s, fraud detection process 10c1, fraud detection process 10c2, fraud detection process 10c3 and/or fraud detection process 10c4 to data acquisition system 12. Examples of IO request 20 may include but are not limited to data write requests (i.e. a request that content be written to data acquisition system 12) and data read requests (i.e. a request that content be read from data acquisition system 12).

[0024] The instruction sets and subroutines of fraud detection process 10c1, fraud detection process 10c2, fraud detection process 10c3 and/or fraud detection process 10c4, which may be stored on storage devices 20, 22, 24, 26 (respectively) coupled to client electronic devices 28, 30, 32, 34 (respectively), may be executed by one or more processors (not shown) and one or more memory architectures (not shown) incorporated into client electronic devices 28, 30, 32, 34 (respectively). Storage devices 20, 22, 24, 26 may include but are not limited to: hard disk drives; optical drives; RAID devices; random access memories (RAM); read-only memories (ROM), and all forms of flash memory storage devices.

[0025] Examples of client electronic devices 28, 30, 32, 34 may include, but are not limited to, data-enabled, cellular telephone 28, laptop computer 30, tablet computer 32, personal computer 34, a notebook computer (not shown), a server computer (not shown),

a gaming console (not shown), a smart television (not shown), and a dedicated network device (not shown). Client electronic devices 28, 30, 32, 34 may each execute an operating system, examples of which may include but are not limited to Microsoft Windows [™], Android [™], WebOS [™], iOS [™], Redhat Linux [™], or a custom operating system.

[0026] Users 36, 38, 40, 42 may access fraud detection process 10 directly through network 14 or through secondary network 18. Further, fraud detection process 10 may be connected to network 14 through secondary network 18, as illustrated with link line 44.

[0027] The various client electronic devices (e.g., client electronic devices 28, 30, 32, 34) may be directly or indirectly coupled to network 14 (or network 18). For example, data-enabled, cellular telephone 28 and laptop computer 30 are shown wirelessly coupled to network 14 via wireless communication channels 46, 48 (respectively) established between data-enabled, cellular telephone 28, laptop computer 30 (respectively) and cellular network / bridge 50, which is shown directly coupled to network 14. Further, tablet computer 32 is shown wirelessly coupled to network 14 via wireless communication channel 52 established between tablet computer 32 and wireless access point (i.e., WAP) 54, which is shown directly coupled to network 14. Additionally, personal computer 34 is shown directly coupled to network 18 via a hardwired network connection.

The Data Acquisition System:

[0028] As will be discussed below in greater detail, data acquisition system 12 may be configured to acquire data that is provided by a third-party (e.g., a caller) to a platform user (e.g., a recipient) during an engagement (e.g., a conversation).

[0029] Examples of such a conversation between a caller (e.g., user 36) and a recipient (e.g., user 42) may include but are not limited to one or more of: a voice-based conversation between the caller (e.g., user 36) and the recipient (e.g., user 42); and a text-based conversation between the caller (e.g., user 36) and the recipient (e.g., user 42). For example, a customer may call a sales phone line to purchase a product; a customer may call a reservation line to book air travel; and a customer may text chat with a customer

service line to request assistance concerning a product purchased or a service received.

[0030] Assume for the following example that the caller (e.g., user 36) is a customer who contacts bank 56 to request assistance concerning one or more of their bank accounts and the recipient (e.g., user 42) is a customer service employee of bank 56.

Fraud Detection Process:

[0031] Referring also to FIG. 2, data acquisition system 12 may monitor the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) to determine whether or not the caller (e.g., user 36) is a fraudster. For the following discussion, a fraudster may be a human being (e.g., a person that commits acts of fraud), a computer-based system (e.g., a speech “bot” that follows a script and uses artificial intelligence to respond to questions by the customer service representative), and a hybrid system (e.g., a person that commits acts of fraud but uses a computer-based system to change their voice).

[0032] In the event that the monitored conversation is a voice-based conversation between the caller (e.g., user 36) and the recipient (e.g., user 42), fraud detection process 10 may process the voice-based conversation to define a conversation transcript for the voice-based conversation. For example, fraud detection process 10 may process the voice-based conversation to produce a conversation transcript using e.g., various speech-to-text platforms or applications (e.g., such as those available from Nuance Communications, Inc. of Burlington, MA).

[0033] Referring also to FIG. 3, there is shown an example of such a conversation transcript between the caller (e.g., user 36) and the recipient (e.g., user 42). In this particular example, the conversation transcript is as follows:

- **User 36:** Hello thank you for calling ABC Bank. My name is Sarah. With whom do I have the pleasure of speaking with today?
- **User 42:** Hi Sarah, this is Martha Haines. How are you doing today?
- **User 36:** I’m fine thank you for asking. Could I ask you to please spell your name for me.

- **User 42:** Martha Haines, H-A-I-N-E-S.
- **User 36:** And what can I do for you today Mrs. Haines.
- **User 42:** I would just like to know the last five transactions on my account please.

(At this point in the conversation, fraud detection process 10 may determine that the caller (i.e., user 42) has passed voice biometrics authentication)

- **User 36:** And which account would you like me to look up?
- **User 42:** My checking account.

(At this point in time, fraud detection process 10 may ask the caller (i.e., user 42) if there is anything else they wanted to do today)

- **User 36:** Sure thing Mrs. Haines, let me pull that right up for you. While I'm looking that up, was there anything else you wanted me to help you with today?
- **User 42:** I also wanted to ask about making a transfer, but only after I see what my account balance is.

(At this point in time, fraud detection process 10 may raise the fraud threat to HIGH)

- **User 36:** I'm so sorry Mrs. Haines, there seems to be a problem with my computer. Please let me transfer you.

[0034] Fraud detection process 10 may receive 100 input information (e.g., input information 58) concerning the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42). Examples of input information 58 received 100 by fraud detection process 10 may include but are not limited to one or more of:

- a caller conversation portion, such as a word, phrase, comment or sentence spoken or typed by the caller (e.g., user 36);
- a recipient conversation portion, such as a word, phrase, comment or

sentence spoken or typed by the recipient (e.g., user 42); and

- biometric information (e.g., biometric information 60), such as inflection patterns, accent patterns, pause patterns, word choice patterns, speech speed patterns, speech cadence patterns, speech rhythm patterns, word length patterns, voice print information, and stress level information concerning the caller (e.g., user 36).

[0035] Specifically and with respect to such biometric information (e.g., biometric information 60), fraud detection process 10 may analyze various speech pattern indicia defined within the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42).

[0036] For example, fraud detection process 10 may process the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) to define one or more inflection patterns of the caller (e.g., user 36). As is known in the art, an inflection is an aspect of speech in which the speaker modifies the pronunciation of a word to express different grammatical categories (such as tense, case, voice, aspect, person, number, gender, and mood). Specifically, certain people may speak in certain manners wherein they may add specific inflections on e.g., the last words of a sentence. Such inflection patterns may be utilized by fraud detection process 10 to identify the provider of such content.

[0037] Additionally, fraud detection process 10 may process the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) to define one or more accent patterns of the caller (e.g., user 36). As is known in the art, different people of different ethnic origins may pronounce the same words differently (e.g., a native-born American speaking English, versus a person from the United Kingdom speaking English, versus a person from India speaking English). Further, people of common ethnic origin may pronounce the same words differently depending upon the particular geographic region in which they are located (e.g., a native-born American from New York City versus a native-born American from Dallas, Texas). Such accent patterns may be utilized by fraud

detection process 10 to identify the provider of such content.

[0038] Further, fraud detection process 10 may process the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) to define one or more pause patterns of the caller (e.g., user 36). As is known in the art, various people speak in various ways. Some people continuously speak without pausing, while other people may introduce a considerable number of pauses into their speech, while others may fill those pauses with filler words (e.g., “ummm”, “you know”, and “like”). Such pause patterns may be utilized by fraud detection process 10 to identify the provider of such content.

[0039] Additionally, fraud detection process 10 may process the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) to define one or more word choice patterns of the caller (e.g., user 36). Specifically, certain people tend to frequently use certain words. For example, one person may frequently use “typically” while another person may frequently use “usually”. Such word choice patterns (e.g., word choice patterns 70) may be utilized by fraud detection process 10 to identify the provider of such content.

[0040] While four specific examples of speech-pattern indicia are described above (namely: inflection patterns, accent patterns, pause patterns, and word choice patterns), this is for illustrative purposes only and is not intended to be a limitation of this disclosure, as other configurations are possible and are considered to be within the scope of this disclosure. Accordingly, other examples of such speech-pattern indicia may include but are not limited to speech speed patterns, speech cadence patterns, speech rhythm patterns, word length patterns, voice print information, stress level information etc. For example, fraud detection process 10 may also utilize question / answer pairings to provide insight as to whether a caller is a fraudster.

[0041] Fraud detection process 10 may process 102 the input information (e.g., input information 58) to assess a fraud-threat-level (e.g., fraud-threat-level 62). For example and when processing 102 the input information (e.g., input information 58) to determine a fraud-threat-level (e.g., fraud-threat-level 62), fraud detection process 10 may determine

104 if the input information (e.g., input information 58) is indicative of fraudulent behavior.

[0042] For example, fraud detection process 10 may determine 104 if a word or phrase (e.g., input information 58) uttered or typed by the caller (e.g., user 36) is indicative of fraudulent behavior. Additionally / alternatively, fraud detection process 10 may determine 104 if biometric information 60 (e.g., inflection patterns, accent patterns, pause patterns, word choice patterns, speech speed patterns, speech cadence patterns, speech rhythm patterns, word length patterns, voice print information, stress level information) associated with the caller (e.g., user 36) is indicative of fraudulent behavior.

[0043] When determining 104 if the input information (e.g., input information 58) is indicative of fraudulent behavior, fraud detection process 10 may compare 106 the input information (e.g., input information 58) to a plurality of fraudulent behaviors (e.g., plurality of fraudulent behaviors 64).

[0044] Referring also to FIG. 4, there is shown a visual example of such a plurality of fraudulent behaviors (e.g., plurality of fraudulent behaviors 64). As shown in this particular example, the items on the left side of the graph (e.g., inquiries about account balances) have a high probability of being fraudulent behavior (90% fraudulent versus 10% legitimate), while the items on the right side of the graph (e.g., requests for help) have a low probability of being fraudulent behavior (10% fraudulent versus 90% legitimate).

[0045] The plurality of fraudulent behaviors (e.g., plurality of fraudulent behaviors 64) may include a plurality of empirically-defined fraudulent behaviors, wherein this plurality of empirically-defined fraudulent behaviors may be defined via AI/ML processing of information concerning a plurality of earlier conversations.

[0046] For example, assume that fraud detection process 10 has access to a data set (e.g., data set 66) that quantifies interactions between customer service representatives and those callers (both legitimate and fraudulent) that reached out to those customer service representatives. For this example, assume that the interactions defined within this data set (e.g., data set 66) identify inquiries made by the callers and the results of the interaction.

Accordingly and by processing such interactions defined within this data set (e.g., data set 66), this plurality of empirically-defined fraudulent behaviors may be defined (via AI/ML processing), resulting in the plurality of fraudulent behaviors 64 defined within FIG. 4.

[0047] Fraud detection process 10 may define 108 a targeted response based, at least in part, upon the fraud-threat-level (e.g., fraud-threat-level 60) assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level (e.g., fraud-threat-level 60). Fraud detection process 10 may then effectuate 110 the targeted response.

[0048] When effectuating 110 the targeted response, fraud detection process 10 may:

- allow 112 the conversation to continue;
- ask 114 a question of the caller (e.g., user 36);
- prompt 116 the recipient (e.g., user 42) to ask a question of the caller (e.g., user 36);
- effectuate 118 a transfer from the recipient (e.g., user 42) to a third-party;
- and
- end 120 the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42).

[0049] For example and if fraud detection process 10 processes 102 the input information (e.g., input information 58) and assesses a fraud-threat-level (e.g., fraud-threat-level 62) that is low, fraud detection process 10 may effectuate 110 a targeted response that allows 112 the conversation to continue. Accordingly and during portion 150 of the conversation transcript shown in FIG. 3, fraud detection process 10 may assess a fraud-threat-level (e.g., fraud-threat-level 62) of low and may allow 112 the conversation to continue.

[0050] Further and if fraud detection process 10 processes 102 the input information (e.g., input information 58) and assesses a fraud-threat-level (e.g., fraud-threat-level 62) that is intermediate, fraud detection process 10 may effectuate 110 a targeted response that asks 114 a question of the caller (e.g., user 36). Accordingly and during portion 152 of the

conversation transcript shown in FIG. 3, fraud detection process 10 may assess a fraud-threat-level (e.g., fraud-threat-level 62) of intermediate and may ask 114 a question of the caller (e.g., user 36). In this particular example, the question asked (“Is there anything else that you would like to do today?”) may be directly asked via a synthesized voice (if a voice-based exchange) or via text (if a text-based exchange).

[0051] Alternatively and if fraud detection process 10 processes 102 the input information (e.g., input information 58) and assesses a fraud-threat-level (e.g., fraud-threat-level 62) that is intermediate, fraud detection process 10 may effectuate 110 a targeted response that prompts 116 the recipient (e.g., user 42) to ask a question of the caller (e.g., user 36). Accordingly and during portion 152 of the conversation transcript shown in FIG. 3, fraud detection process 10 may assess a fraud-threat-level (e.g., fraud-threat-level 62) of intermediate and may prompt 116 a question of the caller (e.g., user 36). In this particular example, the question asked (“Is there anything else that you would like to do today?”) may be indirectly asked via the recipient (e.g., user 42) after prompting by fraud detection process 10.

[0052] Further and if fraud detection process 10 processes 102 the input information (e.g., input information 58) and assesses a fraud-threat-level (e.g., fraud-threat-level 62) that is high, fraud detection process 10 may effectuate 110 a targeted response that effectuates 118 a transfer from the recipient (e.g., user 42) to a third-party. Accordingly and during portion 154 of the conversation transcript shown in FIG. 3, fraud detection process 10 may assess a fraud-threat-level (e.g., fraud-threat-level 62) of high and may effectuate 118 a transfer of the caller (e.g., user 36) from the recipient (e.g., user 42) to a third-party (such as a supervisor or a manager).

[0053] Alternatively and if fraud detection process 10 processes 102 the input information (e.g., input information 58) and assesses a fraud-threat-level (e.g., fraud-threat-level 62) that is high, fraud detection process 10 may effectuate 110 a targeted response that ends 120 the conversation between the caller (e.g., user 36) and the recipient (e.g., user

42). Accordingly and when detecting a fraud-threat-level (e.g., fraud-threat-level 62) of high, fraud detection process 10 may end 120 the conversation between the caller (e.g., user 36) and the recipient (e.g., user 42) by disconnecting the call.

[0054] While described above are five targeted responses that may be effectuated 100 by fraud detection process 10, this is for illustrative purposes only and is not intended to be a limitation of this disclosure, as other configurations are possible and are considered to be within the scope of this disclosure. For example and when effectuating 100 a targeted response, fraud detection process 10 may display a result / decision to the recipient (e.g., user 42); and/or may display a result / decision to a backend analyst (not shown).

General:

[0055] As will be appreciated by one skilled in the art, the present disclosure may be embodied as a method, a system, or a computer program product. Accordingly, the present disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a “circuit,” “module” or “system.” Furthermore, the present disclosure may take the form of a computer program product on a computer-usable storage medium having computer-usable program code embodied in the medium.

[0056] Any suitable computer usable or computer readable medium may be utilized. The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples (a non-exhaustive list) of the computer-readable medium may include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a transmission media such as those

supporting the Internet or an intranet, or a magnetic storage device. The computer-usable or computer-readable medium may also be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory. In the context of this document, a computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer-usable medium may include a propagated data signal with the computer-usable program code embodied therewith, either in baseband or as part of a carrier wave. The computer usable program code may be transmitted using any appropriate medium, including but not limited to the Internet, wireline, optical fiber cable, RF, etc.

[0057] Computer program code for carrying out operations of the present disclosure may be written in an object oriented programming language such as Java, Smalltalk, C++ or the like. However, the computer program code for carrying out operations of the present disclosure may also be written in conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through a local area network / a wide area network / the Internet (e.g., network 14).

[0058] The present disclosure is described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, may be implemented by computer program

instructions. These computer program instructions may be provided to a processor of a general purpose computer / special purpose computer / other programmable data processing apparatus, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0059] These computer program instructions may also be stored in a computer-readable memory that may direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0060] The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0061] The flowcharts and block diagrams in the figures may illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present disclosure. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order,

depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustrations, and combinations of blocks in the block diagrams and/or flowchart illustrations, may be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

[0062] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the disclosure. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0063] The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present disclosure has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the disclosure in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the disclosure. The embodiment was chosen and described in order to best explain the principles of the disclosure and the practical application, and to enable others of ordinary skill in the art to understand the disclosure for various embodiments with various modifications as are suited to the particular use contemplated.

[0064] A number of implementations have been described. Having thus described the disclosure of the present application in detail and by reference to embodiments thereof, it will be apparent that modifications and variations are possible without departing from the

scope of the disclosure defined in the appended claims.

What Is Claimed Is:

1. A computer-implemented method, executed on a computing device, comprising:
 - receiving input information concerning a conversation between a caller and a recipient;
 - processing the input information to assess a fraud-threat-level;
 - defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and
 - effectuating the targeted response.
2. The computer-implemented method of claim 1 wherein the input information includes one or more of:
 - a caller conversation portion;
 - a recipient conversation portion; and
 - biometric information concerning the caller.
3. The computer-implemented method of claim 1 wherein the conversation includes one or more of:
 - a voice-based conversation between the caller and the recipient; and
 - a text-based conversation between the caller and the recipient.
4. The computer-implemented method of claim 1 wherein effectuating the targeted response includes one or more of:
 - allowing the conversation to continue;
 - asking a question of the caller;
 - prompting the recipient to ask a question of the caller;
 - effecting a transfer from the recipient to a third-party; and

ending the conversation between the caller and the recipient.

5. The computer-implemented method of claim 1 wherein processing the input information to determine a fraud-threat-level includes:

determining if the input information is indicative of fraudulent behavior.

6. The computer-implemented method of claim 5 wherein determining if the input information is indicative of fraudulent behavior includes:

comparing the input information to a plurality of fraudulent behaviors.

7. The computer-implemented method of claim 6 wherein the plurality of fraudulent behaviors includes a plurality of empirically-defined fraudulent behaviors.

8. The computer-implemented method of claim 7 wherein the plurality of empirically-defined fraudulent behaviors are defined via AI/ML processing of information concerning a plurality of earlier conversations.

9. A computer program product residing on a computer readable medium having a plurality of instructions stored thereon which, when executed by a processor, cause the processor to perform operations comprising:

receiving input information concerning a conversation between a caller and a recipient;

processing the input information to assess a fraud-threat-level;

defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and

effectuating the targeted response.

10. The computer program product of claim 8 wherein the input information includes one or more of:

- a caller conversation portion;
- a recipient conversation portion; and
- biometric information concerning the caller.

11. The computer program product of claim 8 wherein the conversation includes one or more of:

- a voice-based conversation between the caller and the recipient; and
- a text-based conversation between the caller and the recipient.

12. The computer program product of claim 8 wherein effectuating the targeted response includes one or more of:

- allowing the conversation to continue;
- asking a question of the caller;
- prompting the recipient to ask a question of the caller;
- effecting a transfer from the recipient to a third-party; and
- ending the conversation between the caller and the recipient.

13. The computer program product of claim 8 wherein processing the input information to determine a fraud-threat-level includes:

- determining if the input information is indicative of fraudulent behavior.

14. The computer program product of claim 13 wherein determining if the input information is indicative of fraudulent behavior includes:

- comparing the input information to a plurality of fraudulent behaviors.

15. The computer program product of claim 14 wherein the plurality of fraudulent behaviors includes a plurality of empirically-defined fraudulent behaviors.

16. The computer program product of claim 15 wherein the plurality of empirically-defined fraudulent behaviors are defined via AI/ML processing of information concerning a plurality of earlier conversations.

17. A computing system including a processor and memory configured to perform operations comprising:

receiving input information concerning a conversation between a caller and a recipient;

processing the input information to assess a fraud-threat-level;

defining a targeted response based, at least in part, upon the fraud-threat-level assessed, wherein the targeted response is intended to refine the assessed fraud-threat-level; and

effectuating the targeted response.

18. The computing system of claim 17 wherein the input information includes one or more of:

a caller conversation portion;

a recipient conversation portion; and

biometric information concerning the caller.

19. The computing system of claim 17 wherein the conversation includes one or more of:

a voice-based conversation between the caller and the recipient; and

a text-based conversation between the caller and the recipient.

20. The computing system of claim 17 wherein effectuating the targeted response includes one or more of:

- allowing the conversation to continue;
- asking a question of the caller;
- prompting the recipient to ask a question of the caller;
- effecting a transfer from the recipient to a third-party; and
- ending the conversation between the caller and the recipient.

21. The computing system of claim 17 wherein processing the input information to determine a fraud-threat-level includes:

- determining if the input information is indicative of fraudulent behavior.

22. The computing system of claim 21 wherein determining if the input information is indicative of fraudulent behavior includes:

- comparing the input information to a plurality of fraudulent behaviors.

23. The computing system of claim 22 wherein the plurality of fraudulent behaviors includes a plurality of empirically-defined fraudulent behaviors.

24. The computing system of claim 23 wherein the plurality of empirically-defined fraudulent behaviors are defined via AI/ML processing of information concerning a plurality of earlier conversations.

1/4

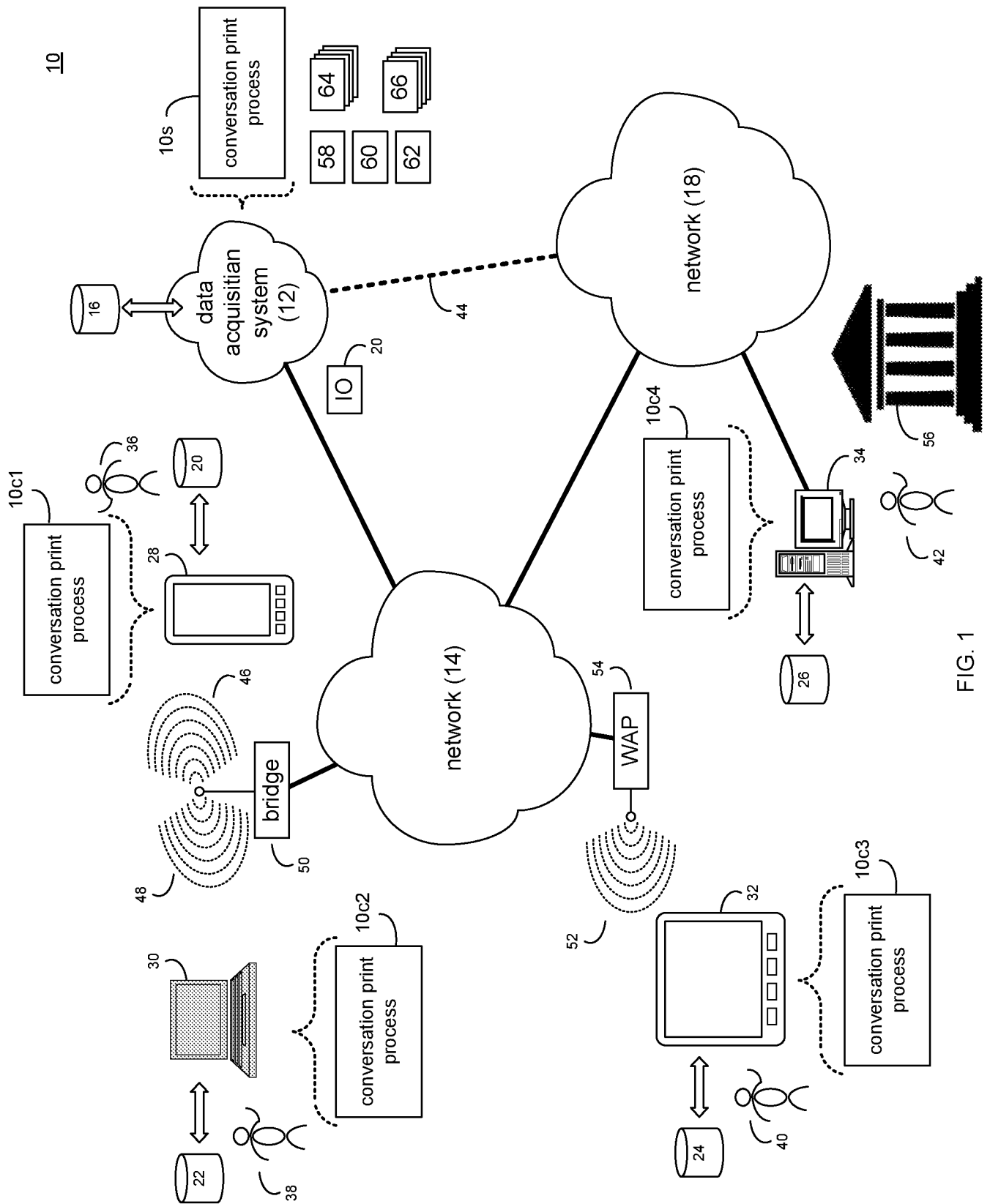


FIG. 1

10

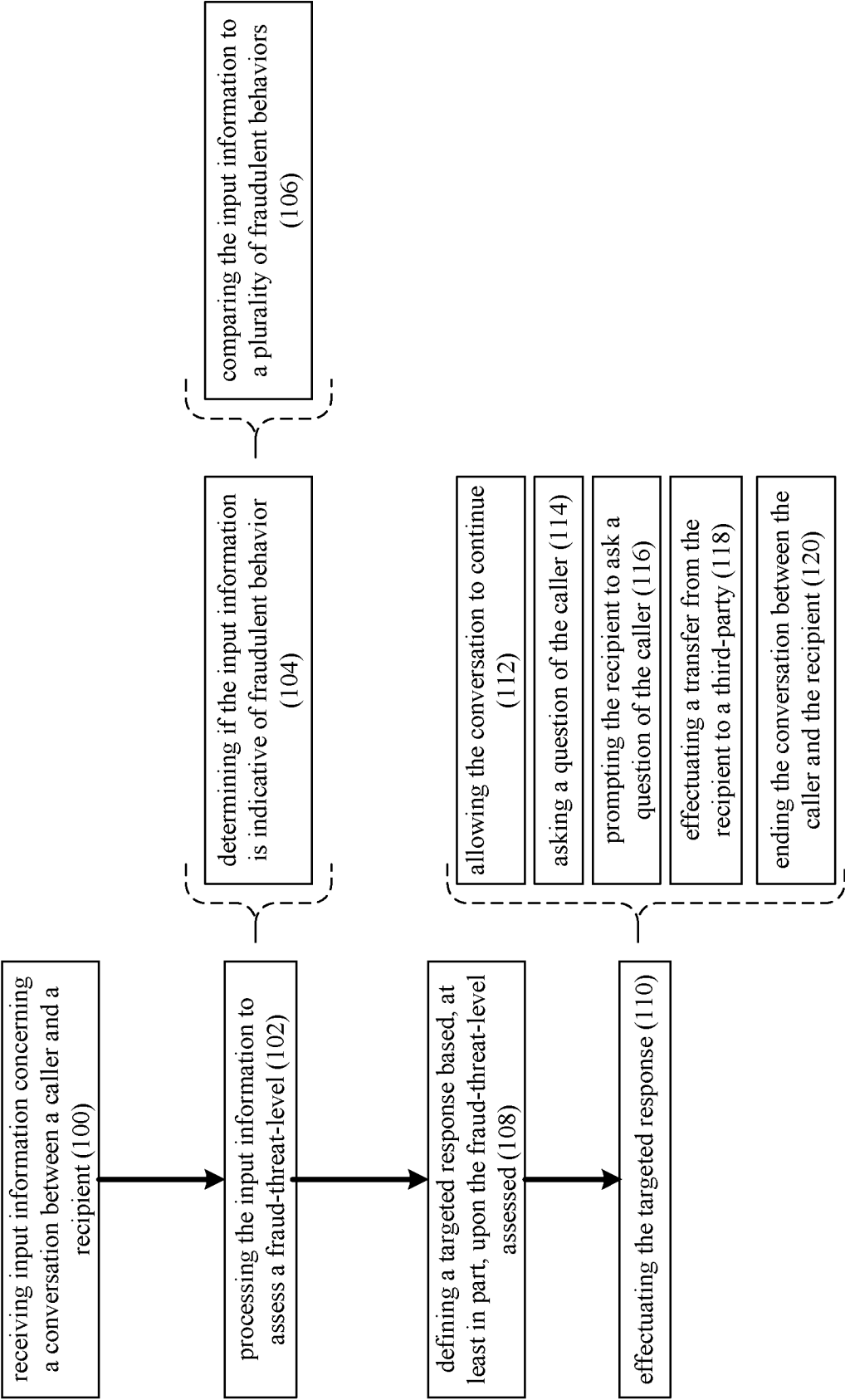


FIG. 2

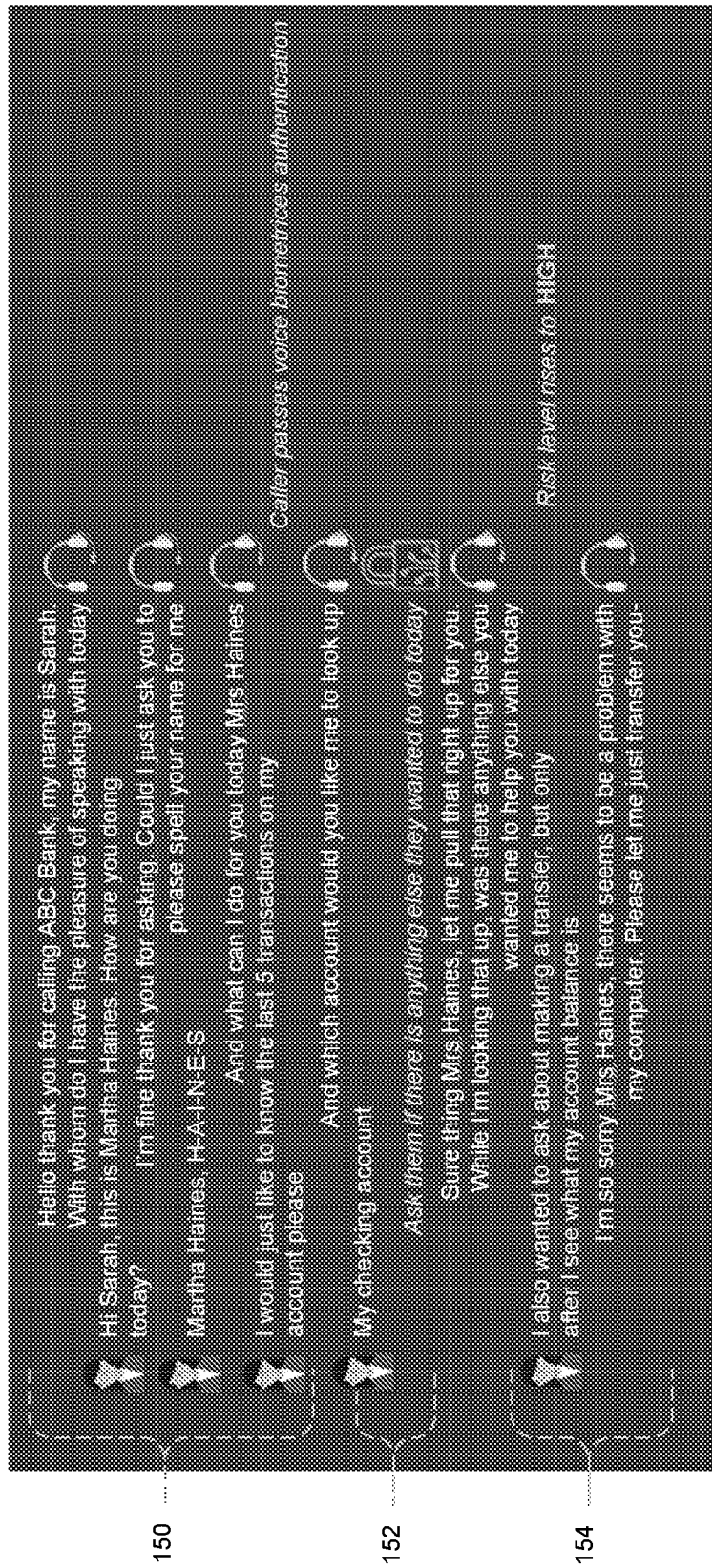


FIG. 3

What Fraudsters are Saying



FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2021/056251**A. CLASSIFICATION OF SUBJECT MATTER**

IPC: H04M 3/42

CPC: H04M 3/42221

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

CPC: H04M 3/42221, 3/2281, 3/42042, 3/42059, 2203/6027

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

USPC: 379/88.02, 88.19, 88.26, 114.14, 144.01

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PGPUB; USPT; USOC; EPAB; JPAB; DWPI; TDBD; Search Terms: fraudster, fraudulent, fraud, behavior, threat, level, caller, calling party, originator, initiator, sender

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/0269946 A1 (JONES) 24 September 2015 (24.09.2015) , entire document.	1-24
A	US 2018/0240028 A1 (BARACALDO ANGEL ET AL.) 23 August 2018 (23.08.2018) , entire document.	1-24

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

30 November 2021 (30.11.2021)

Date of mailing of the international search report

01 December 2021 (01.12.2021)

Name and mailing address of the ISA/US

**COMMISSIONER FOR PATENTS MAIL STOP PCT,
ATTN: ISA/US P.O. BOX 1450 ALEXANDRIA, VA
22313-1450, UNITED STATES OF AMERICA**

Facsimile No. (571)273-8300

Authorized officer

HARRY C. KIM

Telephone No. 571-272-4300