

(51) International Patent Classification:
G06Q 40/00 (2012.01)(21) International Application Number:
PCT/US2013/049045(22) International Filing Date:
2 July 2013 (02.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/541,157 3 July 2012 (03.07.2012) US(71) Applicant: LEXISNEXIS RISK SOLUTIONS FL INC.
[US/US]; 6601 Park of Commerce Boulevard, Boca Raton,
FL 33487 (US).(72) Inventor: BUCHOLZ, Andrew John; 509 Robinson
Court, Alexandria, VA 22302 (US).(74) Agents: JONES, Mark Lehi et al.; Troutman Sanders
LLP, Bank of America Plaza, 600 Peachtree Street, NE,
Suite 5200, Atlanta, GA 30308-2216 (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, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, 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, SC,
SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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).

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR DETECTING TAX REFUND FRAUD

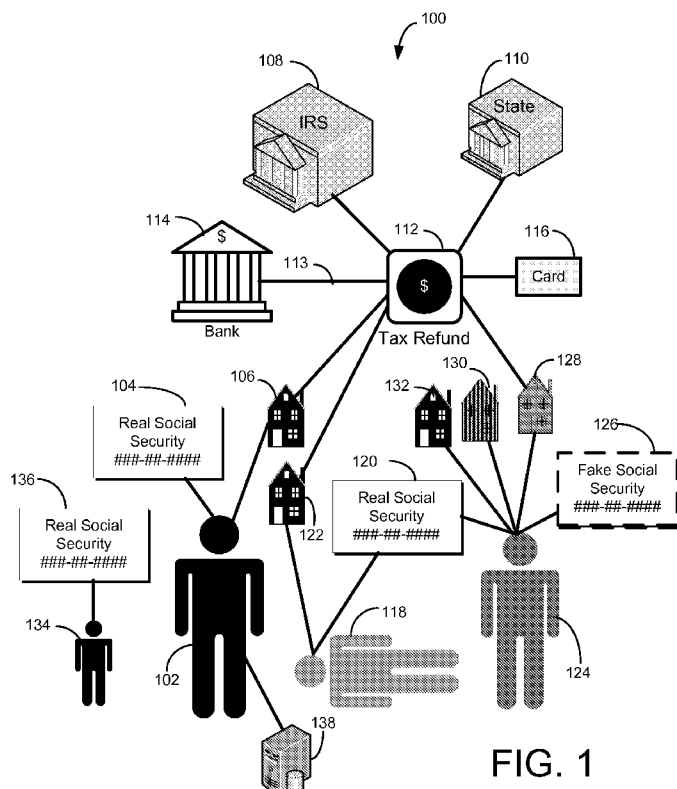


FIG. 1

(57) Abstract: Certain embodiments of the disclosed tech-
nology may include systems and methods for detecting tax
refund fraud. According to an exemplary embodiment of the
disclosed technology, a method is provided for detecting tax
refund fraud. The method includes receiving entity-supplied
information. In an exemplary embodiment, the entity-sup-
plied information includes at least a name, social security
number, and mailing address. The method further includes
querying one or more databases with the entity-supplied in-
formation and receiving a plurality of independent infor-
mation in response to the querying. The method can include de-
termining, based at least in part on a comparison of the en-
tity-supplied information with the plurality of independent
information, zero or more indicators of fraud. The method
can include outputting the zero or more indicators of fraud.

**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:

- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

SYSTEMS AND METHODS FOR DETECTING TAX REFUND FRAUD

FIELD

[0001] The disclosed technology generally relates to detecting fraud, and in particular, to systems and methods for detecting tax refund fraud.

BACKGROUND

[0002] Federal and state revenue departments in the United States face a number of problems associated with fraudulent income tax returns. Fraudsters can apply for tax refunds by misrepresenting their identity, by stealing and using identity information from another individual, or by using an identity of a deceased person. The associated revenue loss to the federal and state can be significant, and the process of verifying the legitimacy returns can create costly delays.

[0003] Technically well-informed fraud perpetrators with sophisticated deception schemes are likely to continue targeting tax revenue entities, particularly if fraud detection and prevention mechanisms are not in place. Balancing the threats of identity fraud with efficient service for legitimate refunds creates a significant challenge for federal and state revenue departments.

BRIEF SUMMARY

[0004] Some or all of the above needs may be addressed by certain embodiments of the disclosed technology. Certain embodiments of the disclosed technology may include systems and methods for detecting tax refund fraud.

[0005] According to an exemplary embodiment of the disclosed technology, a method is provided for detecting tax refund fraud. The method includes receiving entity-supplied information. In an exemplary embodiment, the entity-supplied information includes at least a name, social security number, and mailing address. The method further includes querying one or more databases with the entity-supplied information and receiving a plurality of independent information in response to the querying. The plurality of independent information can include one or more of an indication of whether or not the entity is deceased; independent address

information associated with the entity; address validity information associated with the entity-supplied information; one or more public records associated with the entity-supplied information; or no information.

[0006] According to an exemplary embodiment, the method can include determining, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud. According to certain exemplary embodiments, the indicators of fraud can include one or more of an entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information; entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information; no record of association between the entity-supplied mailing address and any independent address information; relatives address or associates address. The method can include outputting the zero or more indicators of fraud.

[0007] According to an exemplary embodiment of the disclosed technology, another method is provided for detecting tax refund fraud. The method can include receiving entity-supplied information. The entity-supplied information can include at least a name and a social security number. The method includes querying one or more public records with the entity-supplied information. The method includes receiving, based at least on the querying, public data that can include one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number. The method can include querying a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data, and outputting a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

[0008] According to another exemplary embodiment, a system is provided for detecting tax refund fraud. The system includes at least one memory for storing data and computer-executable instructions; and at least one processor configured to access the at least one memory and further configured to execute the computer-executable instructions to receive entity-supplied

information. The entity-supplied information includes at least a name, social security number, and mailing address. The system can query one or more databases with the entity-supplied information. The system can receive a plurality of independent information in response to the querying. The plurality of independent information can include one or more of an indication of whether or not the entity is deceased, independent address information associated with the entity; address validity information associated with the entity-supplied information, one or more public records associated with the entity-supplied information, or no information. The system can determine, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud. The indicators of fraud can include an entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information. The indicators of fraud can include an entity-supplied mailing address that is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information. The indicators of fraud can include no record of association between the entity-supplied mailing address and any independent address information; relatives address or associates address. The system can also output the zero or more indicators of fraud.

[0009] According to another exemplary embodiment, a system is provided for detecting tax refund fraud. The system includes at least one memory for storing data and computer-executable instructions; and at least one processor configured to access the at least one memory and further configured to execute the computer-executable instructions to receive entity-supplied information. The entity-supplied information can include at least a name and a social security number. The system can query one or more public records with the entity-supplied information, and receive, based at least on the querying, public data comprising one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number. The system can query a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data and output a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

[0010] Exemplary embodiments of the disclosed technology can include one or more computer readable media comprising computer-executable instructions that, when executed by one or more processors, configure the one or more processors to perform a method. The method includes receiving entity-supplied information. In an exemplary embodiment, the entity-supplied information includes at least a name, social security number, and mailing address. The method further includes querying one or more databases with the entity-supplied information and receiving a plurality of independent information in response to the querying. The plurality of independent information can include one or more of an indication of whether or not the entity is deceased; independent address information associated with the entity; address validity information associated with the entity-supplied information; one or more public records associated with the entity-supplied information; or no information. According to an exemplary embodiment, the method can include determining, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud. According to certain exemplary embodiments, the indicators of fraud can include one or more of an entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information; entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information; no record of association between the entity-supplied mailing address and any independent address information; relatives address or associates address. The method can include outputting the zero or more indicators of fraud.

[0011] Exemplary embodiments of the disclosed technology can include one or more computer readable media comprising computer-executable instructions that, when executed by one or more processors, configure the one or more processors to perform a method. The method includes The method can include receiving entity-supplied information. The entity-supplied information can include at least a name and a social security number. The method includes querying one or more public records with the entity-supplied information. The method includes receiving, based at least on the querying, public data that can include one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied

social security number. The method can include querying a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data, and outputting a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

[0012] Other embodiments, features, and aspects of the disclosed technology are described in detail herein and are considered a part of the claimed disclosed technologies. Other embodiments, features, and aspects can be understood with reference to the following detailed description, accompanying drawings, and claims.

BRIEF DESCRIPTION OF THE FIGURES

[0013] Reference will now be made to the accompanying figures and flow diagrams, which are not necessarily drawn to scale, and wherein:

[0014] FIG. 1 is a block diagram of illustrative tax refund scenarios, according to exemplary embodiments of the disclosed technology.

[0015] FIG. 2 is a block diagram of an illustrative tax refund fraud detection system 200 according to an exemplary embodiment of the disclosed technology.

[0016] FIG. 3 is a block diagram of an illustrative tax refund fraud detection system architecture 300 according to an exemplary embodiment of the disclosed technology.

[0017] FIG. 4 is a flow diagram of a method 400 according to an exemplary embodiment of the disclosed technology.

[0018] FIG. 5 is a flow diagram of a method 500 according to an exemplary embodiment of the disclosed technology.

DETAILED DESCRIPTION

[0019] Embodiments of the disclosed technology will be described more fully hereinafter with reference to the accompanying drawings, in which embodiments of the disclosed technology are shown. This disclosed technology may, however, be embodied in many different

forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the disclosed technology to those skilled in the art.

[0020] In the following description, numerous specific details are set forth. However, it is to be understood that embodiments of the disclosed technology may be practiced without these specific details. In other instances, well-known methods, structures and techniques have not been shown in detail in order not to obscure an understanding of this description. The term “exemplary” herein is used synonymous with the term “example” and is not meant to indicate excellent or best. References to “one embodiment,” “an embodiment,” “exemplary embodiment,” “various embodiments,” etc., indicate that the embodiment(s) of the disclosed technology so described may include a particular feature, structure, or characteristic, but not every embodiment necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrase “in one embodiment” does not necessarily refer to the same embodiment, although it may.

[0021] As used herein, unless otherwise specified the use of the ordinal adjectives “first,” “second,” “third,” etc., to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0022] Certain embodiments of the disclosed technology may enable detection of tax returns with suspect or fraudulent refund requests. Exemplary embodiments of the disclosed technology may utilize information supplied by the refundee together with information obtained from other sources, such as public or private databases, to determine if the refund request is likely to be fraudulent or legitimate. Various exemplary embodiments of the disclosed technology will now be described with reference to the accompanying figures.

[0023] FIG. 1 shows a block diagram of illustrative tax refund scenarios, according to exemplary embodiments of the disclosed technology. In a normal tax refund scenario, a legitimate taxpayer 102 may submit a federal tax return to the Internal Revenue Service (IRS) 108 and/or a state return to a particular State Revenue Department 110. The legitimate taxpayer 102 may have a legitimate social security number 104 associated with their name. In certain

exemplary embodiments, the legitimate taxpayer 102 may also have a legitimate address 106 associated with their name and/or social security number 104. According to certain exemplary embodiments, one or more databases 138 may be utilized, for example, to verify that the name, social security number 104, and/or address 106 match the identity of the legitimate taxpayer 102. In a typical normal scenario, the legitimate taxpayer 104 may submit the tax refund request with their tax return, and the IRS 108 and/or State Revenue Department 110 may provide the tax refund 112. Accordingly, the tax refund 112 may be dispersed to the legitimate taxpayer 102 by (1) a check mailed to the legitimate address 106; (2) a debit card 116 mailed to the legitimate address 106; or (3) electronic funds transferred 113 to the legitimate taxpayer's 102 bank account 114. In such a scenario, the system may work quickly and efficiently to refund tax overpayment to the legitimate taxpayer 102.

[0024] Unfortunately, there exists other scenarios, as depicted in FIG. 1, where a fraudster 124 may apply for a tax refund 112 using misrepresented or stolen identity information. In one exemplary scenario, the fraudster 124 may apply for a tax refund 112 using a social security number 120 and name associated with a deceased person 118. In certain scenarios, the fraudster 124 may open a bank account 114 in the name of the deceased person 118 and request the refund in the form of an electronic deposit 113. In another scenario, the fraudster 124 may request the refund in the form of a debit card. Each of these scenarios may result in the fraudster 124 obtaining the tax refund without having to present positive identification, for example, as is typically needed to cash tax refund checks.

[0025] In certain scenarios, the fraudster 124 may actually reside at a first address 132, or even in jail 130, but may submit a tax refund request with a second address 128 to avoid being tracked down. In certain scenarios, the fraudster 124 may provide a fabricated social security number 126 in requesting the refund. In yet another scenario, the fraudster 126 may steal the real social security number 136 associated with a child 134 to obtain a tax refund.

[0026] Exemplary embodiments of the disclosed technology may be utilized to detect a potential fraudulent tax refund request, and may be utilized to cancel a refund payment to a potential fraudster 124. Other exemplary embodiments of the disclosed technology may be utilized to detect false positive situations and allow refunds for scenarios that may otherwise be

flagged as being suspicious. For example, a legitimate scenario that can appear as fraudulent involves taxable income from a first job. Typically, such taxpayers in this category may be minors with no public record associated with a residence or prior income. Embodiments of the disclosed technology may utilize social security number patterns, blocks, etc., and/or the age of the refundee to determine legitimate tax refund requests.

[0027] According to certain exemplary embodiments of the disclosed technology, a potential refundee entity may provide certain entity-supplied information with a tax return or refund request that includes at least a name, social security number, and mailing address. In an exemplary embodiment, one or more databases may be queried with the entity-supplied information. For example, the one or more databases may include public or private databases. In accordance with certain exemplary embodiments, one or more public records may be utilized to verify entity-supplied information or retrieve additional information based on the entity-supplied information. According to exemplary embodiments, the public records may include one or more of housing records, vehicular records, marriage records, divorce records, hospital records, death records, court records, property records, incarceration records, or utility records. In exemplary embodiments, the utility records can include one or more of utility hookups, disconnects, and associated service addresses.

[0028] According to exemplary embodiments, a plurality of independent information may be received in response to the querying of the public or private database(s). In accordance with exemplary embodiments, the independent information may include, but is not limited to (1) an indication of whether or not the entity is deceased; (2) independent address information associated with the entity; (3) address validity information associated with the entity-supplied information; (3) one or more public records associated with the entity-supplied information; or (4) no information.

[0029] Exemplary embodiments of the disclosed technology may make a comparison of the entity-supplied information with the plurality of independent information to determine zero or more indicators of fraud. For example, embodiments of the disclosed technology may compare the entity-supplied information with the plurality of independent information to determine if the entity died within tax year, or if the entity died within a timeframe of the tax year that would

indicate a possible non-fraud tax refund request, but with no record of association between the entity-supplied mailing address and the address information obtained via the independent information. Such a scenario may represent a situation where a fraudster 124 has obtained a name and social security information 120 from a deceased person 118, but where the address provided does not correspond with the known residence address 122 of the deceased person 118, or with any known relatives or associates of the deceased person 118. This scenario may be an indicator of a attempt by a fraudster 124 to have a deceased person's 118 tax refund 112 sent to a post office box or other address that can be monitored by the fraudster 124 without any direct tie to the fraudster 124. Exemplary embodiments of the disclosed technology may include a length of time entity has been deceased (if the entity is deceased) in the determination of fraud indicators. For example, a tax refund request listing a person known to be dead for 10 years is very likely a fraudulent refund request.

[0030] According to another exemplary embodiment of the disclosed technology, a comparison may be made with the entity-supplied mailing address and the independent information to determine if the entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information. For example, situations exist where a legitimate taxpayer 102 may abbreviate or include a typographical error their return mailing address, but they may provide a correct zip code that could be verified with the independent information. However, a fraudster 124 may be likely to use a completely different zip code, and in such situations, embodiments of the disclosed technology may utilize the inconsistent zip code information to flag a possible fraudulent tax return request.

[0031] According to another exemplary embodiment of the disclosed technology, a comparison may be made with the entity-supplied mailing address and the independent information to determine whether or not there is any record of association between the entity-supplied mailing address and any independent address information, such as the address of a relative, or associate. According to an exemplary embodiment, if there is no association between the entity-supplied mailing address and any independent address information, then there is a high likelihood that the refund request is fraudulent.

[0032] In accordance with certain exemplary embodiments of the disclosed technology, fraud false positive indicators may be determined, based at least in part on a comparison of the entity-supplied information with the plurality of independent information. Absent of exemplary embodiments of the disclosed technology, certain situations may be incorrectly flagged as fraudulent, and may create costly and unnecessary refund delays. In one exemplary embodiment, a fraud false positive indicator may be based on an analysis to detect if the entity-supplied mailing address is invalid, but with a record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information. This represents a situation where a legitimate taxpayer 102 has abbreviated their address or included a typographical error in the address, but the zip code corresponds with one known to be associated with the legitimate taxpayer 102.

[0033] According to another exemplary embodiment, a fraud false positive indicator may be based on the entity-supplied social security number when there is no independent information available. For example, in one exemplary embodiment, the entity-supplied social security number may be checked to determine if it is valid and issued within 3 to 15 years, and the independent information can be checked to see if it includes information. If no independent information is available and if the entity-supplied social security number is valid and issued within 3 to 15 years, then this information may provide an indication that the entity is a minor. In another exemplary embodiment, the social security number may be checked to determine if the entity is at least 24 years old with a valid social security number issued within 3 to 15 years, and the obtained independent information includes no information. In this scenario, exemplary embodiments of the disclosed technology may provide an indication that the entity is an immigrant.

[0034] According to exemplary embodiments of the disclosed technology, one or more public or private databases 138 may be accessed to receive independent information. For example, one or more public records may be provided housing records, vehicular records, marriage records, divorce records, hospital records, death records, court records, property records, incarceration records, or utility records. In exemplary embodiments, the utility records may include one or more of utility hookups, disconnects, and associated service addresses. According to exemplary embodiments of the disclosed technology, such public records may be

searched by social security number and/or name to provide independent information that can be utilized to verify entity-supplied information. For example, entity-supplied address information can be checked to determine if it corresponds to any addresses of relatives or associates of the entity.

[0035] According to certain exemplary embodiments of the disclosed technology, tax refund fraud may be detected by querying a Do Not Pay list with a combination of entity-supplied information and independent information obtained from one or more public records. For example, a person may be listed on a Do Not Pay list for a number of reasons, including being incarcerated, not paying child support, having liens, etc. Persons on the Do Not Pay list may supply an incorrect social security number or a slight misspelling of a name to avoid being matched with the information on the Do Not Pay list. Therefore, exemplary embodiments of the disclosed technology may include receiving entity-supplied information that includes at least a name and a social security number and querying one or more public records with the entity-supplied information. Exemplary embodiments of the disclosed technology may receive, based at least on the querying, public data that includes one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number. According to exemplary embodiments of the disclosed technology, a Do Not Pay list may be queried with one or more combinations of the entity-supplied information and the received public data and a fraud alert may be output if the one or more combinations result in a match with at least one record in the Do Not Pay list.

[0036] According to certain exemplary embodiments, the Do Not Pay list may be queried with one or more combinations of the entity-supplied name and entity-supplied social security number, the entity-supplied name and the second social security number, the second name or name variant and the entity supplied social security number, or the second name or name variant and the second social security number. According to exemplary embodiments, if one of the combinations matches the information on the Do Not Pay list, then a fraud alert may be output.

[0037] FIG. 2 depicts a block diagram of an illustrative tax refund fraud detection system 200 according to an exemplary embodiment of the disclosed technology. The system 200

includes a controller 202 that includes a memory 204, one or more processors 206, an input/output interface 208 for communicating with a local monitor 218 and input devices, and one or more network interfaces 210 for communicating with local or remote servers or databases 222, which may be accessed through a local area network or the internet 220. According to exemplary embodiments, the memory may included an operating system 212, data 214, and one or more tax refund fraud analysis modules 216.

[0038] Various embodiments of the communication systems and methods herein may be embodied in non-transitory computer readable media for execution by a processor. An exemplary embodiment may be used in an application of a mobile computing device, such as a smartphone or tablet, but other computing devices may also be used. FIG. 3 illustrates schematic diagram of internal architecture of an exemplary mobile computing device 300. It will be understood that the architecture illustrated in FIG. 3 is provided for exemplary purposes only and does not limit the scope of the various embodiments of the communication systems and methods.

[0039] FIG. 3 depicts a block diagram of an illustrative computer system architecture 300 according to an exemplary embodiment of the disclosed technology. Certain aspects of FIG. 3 may also be embodied in the controller 202, as shown in FIG. 2. Various embodiments of the communication systems and methods herein may be embodied in non-transitory computer readable media for execution by a processor. It will be understood that the architecture illustrated in FIG. 3 is provided for exemplary purposes only and does not limit the scope of the various embodiments of the communication systems and methods.

[0040] The architecture 300 of FIG. 3 includes a central processing unit (CPU) 302, where computer instructions are processed; a display interface 304 that acts as a communication interface and provides functions for rendering video, graphics, images, and texts on the display; a keyboard interface 306 that provides a communication interface to a keyboard; and a pointing device interface 308 that provides a communication interface to a pointing device or touch screen. Exemplary embodiments of the architecture 300 may include an antenna interface 310 that provides a communication interface to an antenna; a network connection interface 312 that provides a communication interface to a network. In certain embodiments, a camera interface 314 is provided that acts as a communication interface and provides functions for capturing

digital images from a camera. In certain embodiments, a sound interface 316 is provided as a communication interface for converting sound into electrical signals using a microphone and for converting electrical signals into sound using a speaker. According to exemplary embodiments, a random access memory (RAM) 318 is provided, where computer instructions and data are stored in a volatile memory device for processing by the CPU 302.

[0041] According to an exemplary embodiment, the architecture 300 includes a read-only memory (ROM) 320 where invariant low-level systems code or data for basic system functions such as basic input and output (I/O), startup, or reception of keystrokes from a keyboard are stored in a non-volatile memory device. According to an exemplary embodiment, the architecture 300 includes a storage medium 322 or other suitable type of memory (e.g. such as RAM, ROM, programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic disks, optical disks, floppy disks, hard disks, removable cartridges, flash drives), where the files include an operating system 324, application programs 326 (including, for example, a web browser application, a widget or gadget engine, and or other applications, as necessary) and data files 328 are stored. According to an exemplary embodiment, the architecture 300 includes a power source 330 that provides an appropriate alternating current (AC) or direct current (DC) to power components. According to an exemplary embodiment, the architecture 300 includes and a telephony subsystem 332 that allows the device 300 to transmit and receive sound over a telephone network. The constituent devices and the CPU 302 communicate with each other over a bus 334.

[0042] In accordance with exemplary embodiments, the CPU 302 has appropriate structure to be a computer processor. In one arrangement, the computer CPU 302 is more than one processing unit. The RAM 318 interfaces with the computer bus 334 to provide quick RAM storage to the CPU 302 during the execution of software programs such as the operating system application programs, and device drivers. More specifically, the CPU 302 loads computer-executable process steps from the storage medium 322 or other media into a field of the RAM 318 in order to execute software programs. Data is stored in the RAM 318, where the data is accessed by the computer CPU 302 during execution. In one exemplary configuration, the device 300 includes at least 128 MB of RAM, and 256 MB of flash memory.

[0043] The storage medium 322 itself may include a number of physical drive units, such as a redundant array of independent disks (RAID), a floppy disk drive, a flash memory, a USB flash drive, an external hard disk drive, thumb drive, pen drive, key drive, a High-Density Digital Versatile Disc (HD-DVD) optical disc drive, an internal hard disk drive, a Blu-Ray optical disc drive, or a Holographic Digital Data Storage (HDDS) optical disc drive, an external mini-dual in-line memory module (DIMM) synchronous dynamic random access memory (SDRAM), or an external micro-DIMM SDRAM. Such computer readable storage media allow the device 300 to access computer-executable process steps, application programs and the like, stored on removable and non-removable memory media, to off-load data from the device 300 or to upload data onto the device 300. A computer program product, such as one utilizing a communication system may be tangibly embodied in storage medium 322, which may comprise a machine-readable storage medium.

[0044] An exemplary method 400 for detecting tax refund fraud will now be described with reference to the flowchart of FIG. 4. The method 400 starts in block 402, and according to an exemplary embodiment of the disclosed technology includes receiving entity-supplied information comprising at least a name, social security number, and mailing address. In block 404, the method 400 includes querying one or more databases with the entity-supplied information. In block 406, the method 400 includes receiving a plurality of independent information in response to the querying. In an exemplary embodiment, the plurality of independent information includes one or more of an indication of whether or not the entity is deceased; independent address information associated with the entity; address validity information associated with the entity-supplied information; one or more public records associated with the entity-supplied information; or no information. In block 408, the method 400 includes determining, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud. According to exemplary embodiments, the zero or more indicators of fraud can include one or more of an entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information; entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information; or no record of

association between the entity-supplied mailing address and any independent address information; relatives address or associates address; and. In block 410, the method 400 includes outputting the zero or more indicators of fraud. The method 400 ends after block 410.

[0045] Another exemplary method 500 for detecting tax refund fraud will now be described with reference to the flowchart of FIG. 5. The method 500 starts in block 502, and according to an exemplary embodiment of the disclosed technology includes receiving entity-supplied information comprising at least a name and a social security number. In block 504, the method 500 includes querying one or more public records with the entity-supplied information. In block 506, the method 500 includes receiving, based at least on the querying, public data. The public data can include one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number. In block 508, the method 500 includes querying a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data. In block 510, the method 500 includes outputting a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list. The method 500 ends after block 510.

[0046] According to exemplary embodiments, certain technical effects can be provided, such as creating certain systems and methods that detect tax refund fraud. Exemplary embodiments of the disclosed technology can provide the further technical effects of providing systems and methods for determining and eliminating false positives with respect to tax refund fraud, thereby increasing the efficiency of the tax refund systems.

[0047] In exemplary embodiments of the disclosed technology, the tax refund fraud detection system 200 and/or the tax refund fraud detection system architecture 300 may include any number of hardware and/or software applications that are executed to facilitate any of the operations. In exemplary embodiments, one or more I/O interfaces may facilitate communication between the tax refund fraud detection system 200 and/or the tax refund fraud detection system architecture 300 and one or more input/output devices. For example, a universal serial bus port, a serial port, a disk drive, a CD-ROM drive, and/or one or more user interface devices, such as a display, keyboard, keypad, mouse, control panel, touch screen

display, microphone, etc., may facilitate user interaction with the tax refund fraud detection system 200 and/or the tax refund fraud detection system architecture 300. The one or more I/O interfaces may be utilized to receive or collect data and/or user instructions from a wide variety of input devices. Received data may be processed by one or more computer processors as desired in various embodiments of the disclosed technology and/or stored in one or more memory devices.

[0048] One or more network interfaces may facilitate connection of the tax refund fraud detection system 200 and/or the tax refund fraud detection system architecture 300 inputs and outputs to one or more suitable networks and/or connections; for example, the connections that facilitate communication with any number of sensors associated with the system. The one or more network interfaces may further facilitate connection to one or more suitable networks; for example, a local area network, a wide area network, the Internet, a cellular network, a radio frequency network, a Bluetooth™ enabled network, a Wi-Fi™ enabled network, a satellite-based network any wired network, any wireless network, etc., for communication with external devices and/or systems.

[0049] As desired, embodiments of the disclosed technology may include the tax refund fraud detection system 200 and/or the tax refund fraud detection system architecture 300 with more or less of the components illustrated in FIG. 2 and FIG. 3.

[0050] Certain embodiments of the disclosed technology are described above with reference to block and flow diagrams of systems and methods and/or computer program products according to exemplary embodiments of the disclosed technology. It will be understood that one or more blocks of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and flow diagrams, respectively, can be implemented by computer-executable program instructions. Likewise, some blocks of the block diagrams and flow diagrams may not necessarily need to be performed in the order presented, or may not necessarily need to be performed at all, according to some embodiments of the disclosed technology.

[0051] These computer-executable program instructions may be loaded onto a general-purpose computer, a special-purpose computer, a processor, or other programmable data processing apparatus to produce a particular machine, such that the instructions that execute on

the computer, processor, or other programmable data processing apparatus create means for implementing one or more functions specified in the flow diagram block or blocks. These computer program instructions may also be stored in a computer-readable memory that can 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 that implement one or more functions specified in the flow diagram block or blocks. As an example, embodiments of the disclosed technology may provide for a computer program product, comprising a computer-usable medium having a computer-readable program code or program instructions embodied therein, said computer-readable program code adapted to be executed to implement one or more functions specified in the flow diagram block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational elements or steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions that execute on the computer or other programmable apparatus provide elements or steps for implementing the functions specified in the flow diagram block or blocks.

[0052] Accordingly, blocks of the block diagrams and flow diagrams support combinations of means for performing the specified functions, combinations of elements or steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that each block of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and flow diagrams, can be implemented by special-purpose, hardware-based computer systems that perform the specified functions, elements or steps, or combinations of special-purpose hardware and computer instructions.

[0053] While certain embodiments of the disclosed technology have been described in connection with what is presently considered to be the most practical and various embodiments, it is to be understood that the disclosed technology is not to be limited to the disclosed embodiments, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

[0054] This written description uses examples to disclose certain embodiments of the disclosed technology, including the best mode, and also to enable any person skilled in the art to practice certain embodiments of the disclosed technology, including making and using any devices or systems and performing any incorporated methods. The patentable scope of certain embodiments of the disclosed technology is defined in the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal language of the claims.

CLAIMS

We claim:

1. A computer-implemented method for detecting tax refund fraud, the method comprising:
receiving entity-supplied information comprising at least a name, social security number,
and mailing address;

querying one or more databases with the entity-supplied information;

receiving a plurality of independent information in response to the querying, wherein the
plurality of independent information comprises one or more of:

an indication of whether or not the entity is deceased;

independent address information associated with the entity;

address validity information associated with the entity-supplied information;

one or more public records associated with the entity-supplied information; or

no information; and

determining, based at least in part on a comparison of the entity-supplied information
with the plurality of independent information, zero or more indicators of fraud comprising one or
more of:

entity deceased within tax year or died within a timeframe of the tax year that
would indicate a possible non-fraud tax refund request with no record of association between the
entity-supplied mailing address and the independent address information;

entity-supplied mailing address is invalid with no record of association between a
zip code of the entity-supplied mailing address and one or more zip codes associated with the
independent address information;

no record of association between the entity-supplied mailing address and any
independent address information; relatives address or associates address; and

outputting the zero or more indicators of fraud.

2. The method of claim 1, further comprising:

determining, based at least in part on a comparison of the entity-supplied information
with the plurality of independent information, zero or more fraud false positive indicators
comprising one or more of:

entity-supplied mailing address is invalid with a record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information;

an estimated minor, wherein the entity-supplied social security number is valid and issued within 3 to 15 years or the entity is at least 24 years old, and the independent information comprises no information; and

outputting the or the zero or more fraud false positive indicators.

3. The method of claim 1, wherein, the indication of whether or not the entity is deceased comprises a length of time entity has been deceased if the entity is deceased.

4. The method of claim 1, wherein receiving independent information comprises receiving the one or more public records comprising one or more of housing records, vehicular records, marriage records, divorce records, hospital records, death records, court records, property records, incarceration records, or utility records, wherein the utility records comprise one or more of utility hookups, disconnects, and associated service addresses.

5. The method of claim 1, wherein receiving the address information comprises receiving one or more addresses of relatives or associates of the entity.

6. The method of claim 1, wherein querying one or more databases comprises querying one or more public or private databases.

7. A computer-implemented method for detecting tax refund fraud, the method comprising: receiving entity-supplied information comprising at least a name and a social security number;

querying one or more public records with the entity-supplied information;

receiving, based at least on the querying, public data comprising one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number;

querying a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data; and

outputting a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

8. The computer-implemented method of claim 7, wherein querying the Do Not Pay list with one or more combinations comprises querying the Do Not Pay list with one or more of the entity-supplied name and a the entity-supplied social security number, the entity-supplied name and the second social security number, the second name or name variant and the entity supplied social security number, or the second name or name variant and the second social security number.

9. A system comprising:

at least one memory for storing data and computer-executable instructions; and at least one processor configured to access the at least one memory and further configured to execute the computer-executable instructions to:

receive entity-supplied information comprising at least a name, social security number, and mailing address;

query one or more databases with the entity-supplied information;

receive a plurality of independent information in response to the querying, wherein the plurality of independent information comprises one or more of:

an indication of whether or not the entity is deceased;

independent address information associated with the entity;

address validity information associated with the entity-supplied information;

one or more public records associated with the entity-supplied information; or

no information; and

determine, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud comprising one or more of:

entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information;

entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information;

no record of association between the entity-supplied mailing address and any independent address information; relatives address or associates address; and

output the zero or more indicators of fraud.

10. The system of claim 9, wherein the at least one processor is further configured to execute the computer-executable instructions to:

determine, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more fraud false positive indicators comprising one or more of:

entity-supplied mailing address is invalid with a record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information;

an estimated minor, wherein the entity-supplied social security number is valid and issued within 3 to 15 years or the entity is at least 24 years old, and the independent information comprises no information; and

output the or the zero or more fraud false positive indicators.

11. The system of claim 9, wherein, the indication of whether or not the entity is deceased comprises a length of time entity has been deceased if the entity is deceased.

12. The system of claim 9, wherein the independent information comprises one or more of housing records, vehicular records, marriage records, divorce records, hospital records, death records, court records, property records, incarceration records, or utility records, wherein the utility records comprise one or more of utility hookups, disconnects, and associated service addresses.

13. The system of claim 9, wherein the address information comprises one or more addresses of relatives or associates of the entity.

14. The system of claim 9, wherein the one or more databases comprise one or more public or private databases.

15. A system comprising:

at least one memory for storing data and computer-executable instructions; and at least one processor configured to access the at least one memory and further configured to execute the computer-executable instructions to:

receive entity-supplied information comprising at least a name and a social security number;

query one or more public records with the entity-supplied information;

receive, based at least on the querying, public data comprising one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number;

query a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data; and

output a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

16. The system of claim 15, wherein the one or more combinations of the entity-supplied information and the received public data comprises one or more of the entity-supplied name and a the entity-supplied social security number, the entity-supplied name and the second social security number, the second name or name variant and the entity supplied social security number, or the second name or name variant and the second social security number.

17. One or more computer readable media comprising computer-executable instructions that, when executed by one or more processors, configure the one or more processors to:

receive entity-supplied information comprising at least a name, social security number, and mailing address;

query one or more databases with the entity-supplied information;

receive a plurality of independent information in response to the querying, wherein the plurality of independent information comprises one or more of:

an indication of whether or not the entity is deceased;

independent address information associated with the entity;

address validity information associated with the entity-supplied information;

one or more public records associated with the entity-supplied information; or
no information; and

determine, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more indicators of fraud comprising one or more of:

entity deceased within tax year or died within a timeframe of the tax year that would indicate a possible non-fraud tax refund request with no record of association between the entity-supplied mailing address and the independent address information;

entity-supplied mailing address is invalid with no record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information;

no record of association between the entity-supplied mailing address and any independent address information; relatives address or associates address; and

output the zero or more indicators of fraud.

18. The computer readable media of claim 17, further comprising computer-executable instructions that, when executed by one or more processors, configure the one or more processors to:

determine, based at least in part on a comparison of the entity-supplied information with the plurality of independent information, zero or more fraud false positive indicators comprising one or more of:

entity-supplied mailing address is invalid with a record of association between a zip code of the entity-supplied mailing address and one or more zip codes associated with the independent address information;

an estimated minor, wherein the entity-supplied social security number is valid and issued within 3 to 15 years or the entity is at least 24 years old, and the independent information comprises no information; and

output the or the zero or more fraud false positive indicators.

19. One or more computer readable media comprising computer-executable instructions that, when executed by one or more processors, configure the one or more processors to:

receive entity-supplied information comprising at least a name and a social security number;

query one or more public records with the entity-supplied information;

receive, based at least on the querying, public data comprising one or more of a second social security number associated with entity-supplied name, a second name associated with the entity-supplied social security number, or a name variant associated with the entity-supplied social security number;

query a Do Not Pay list with one or more combinations of the entity-supplied information and the received public data; and

output a fraud alert if the one or more combinations result in a match with at least one record in the Do Not Pay list.

20. The computer readable media of claim 19, wherein the one or more combinations of the entity-supplied information and the received public data comprises one or more of the entity-supplied name and a the entity-supplied social security number, the entity-supplied name and the second social security number, the second name or name variant and the entity supplied social security number, or the second name or name variant and the second social security number.

1 / 5

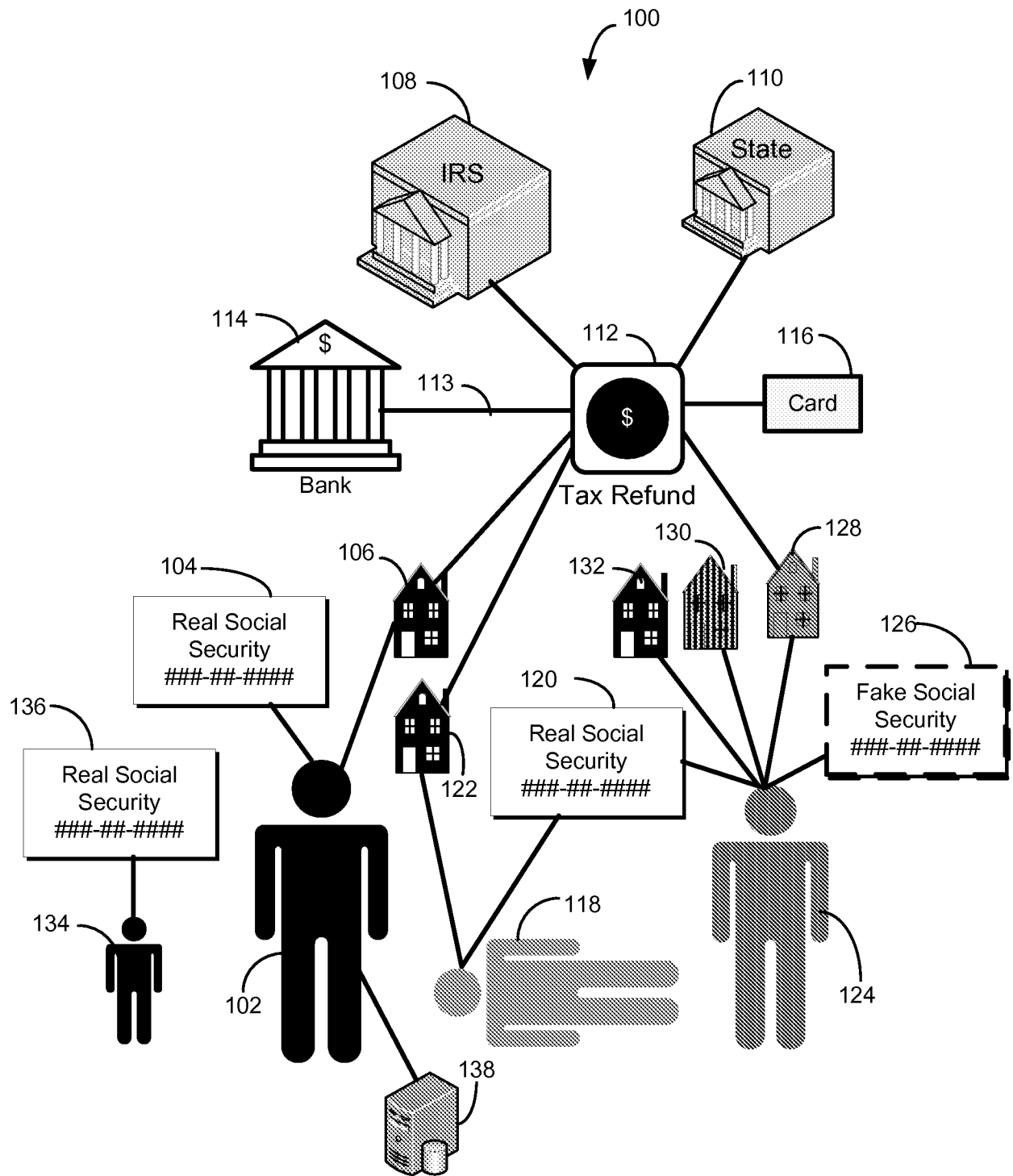


FIG. 1

2 / 5

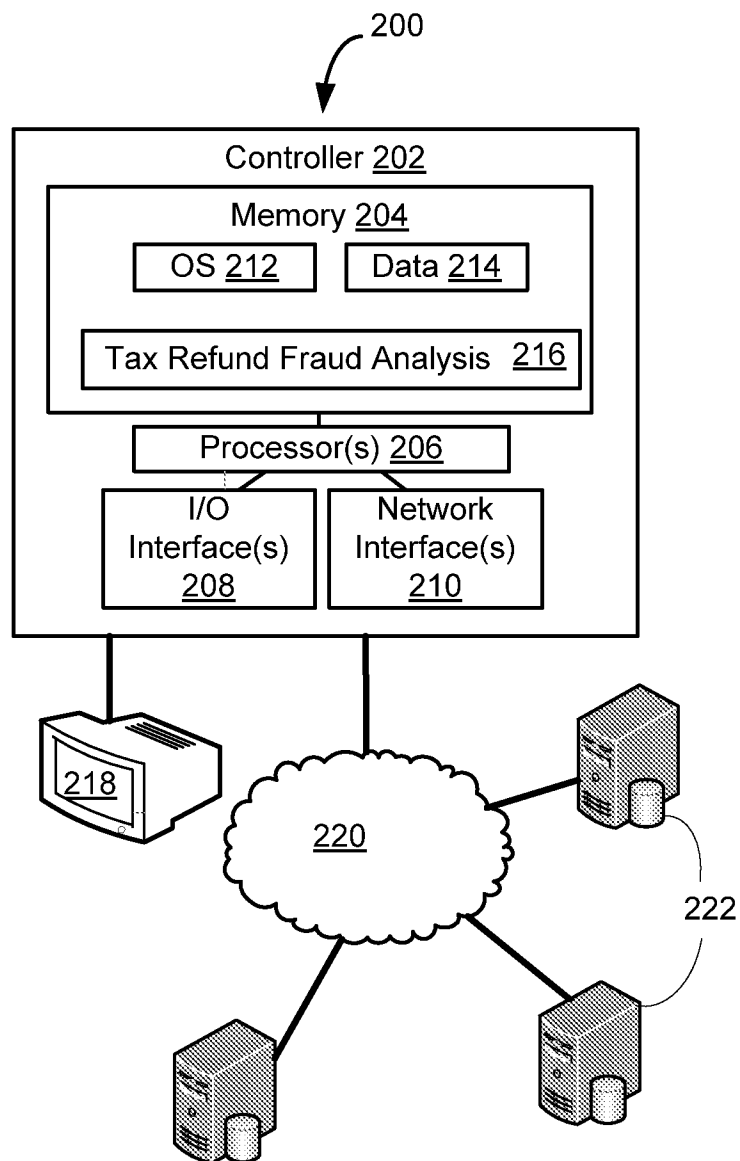


FIG. 2

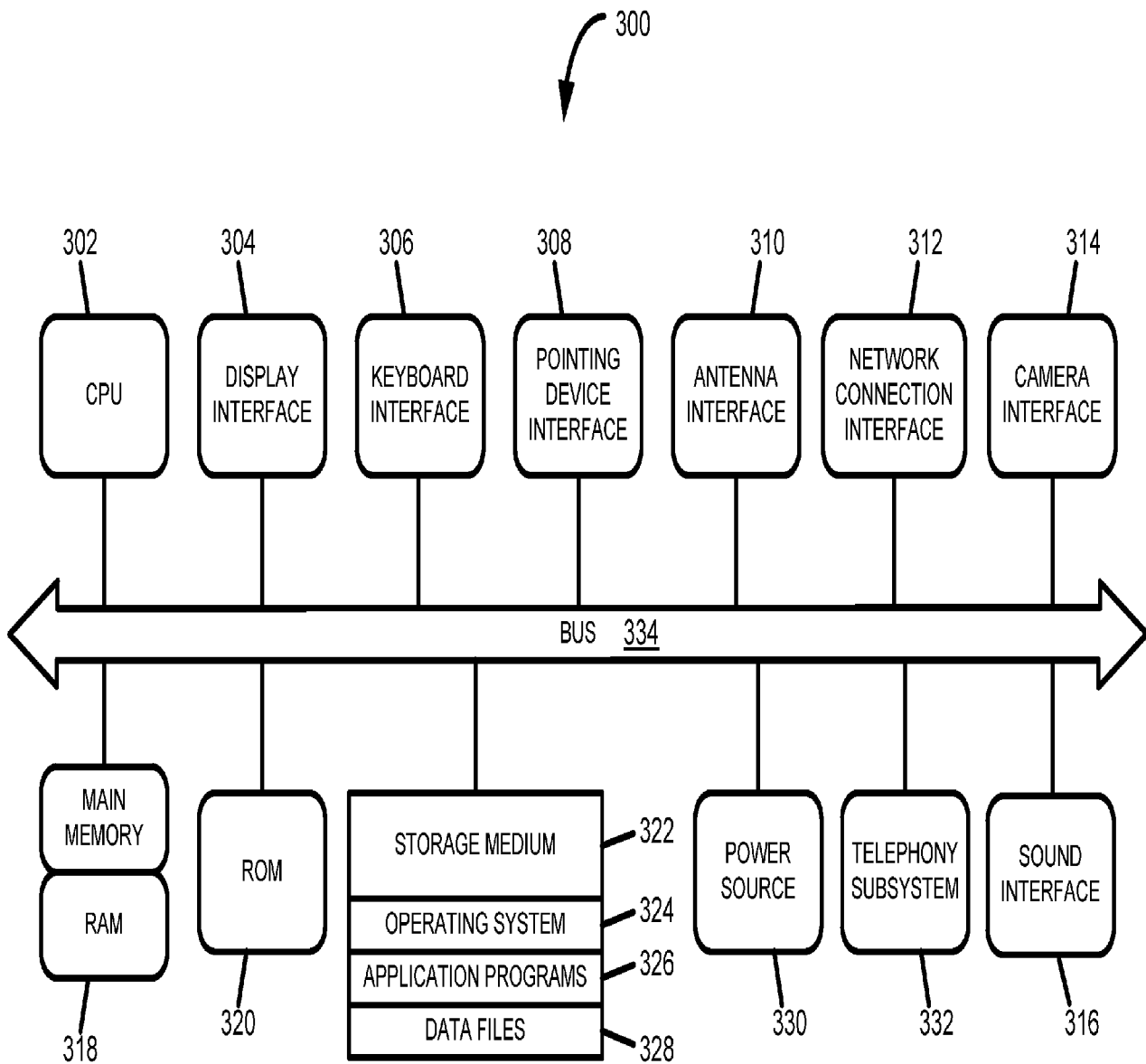


FIG. 3

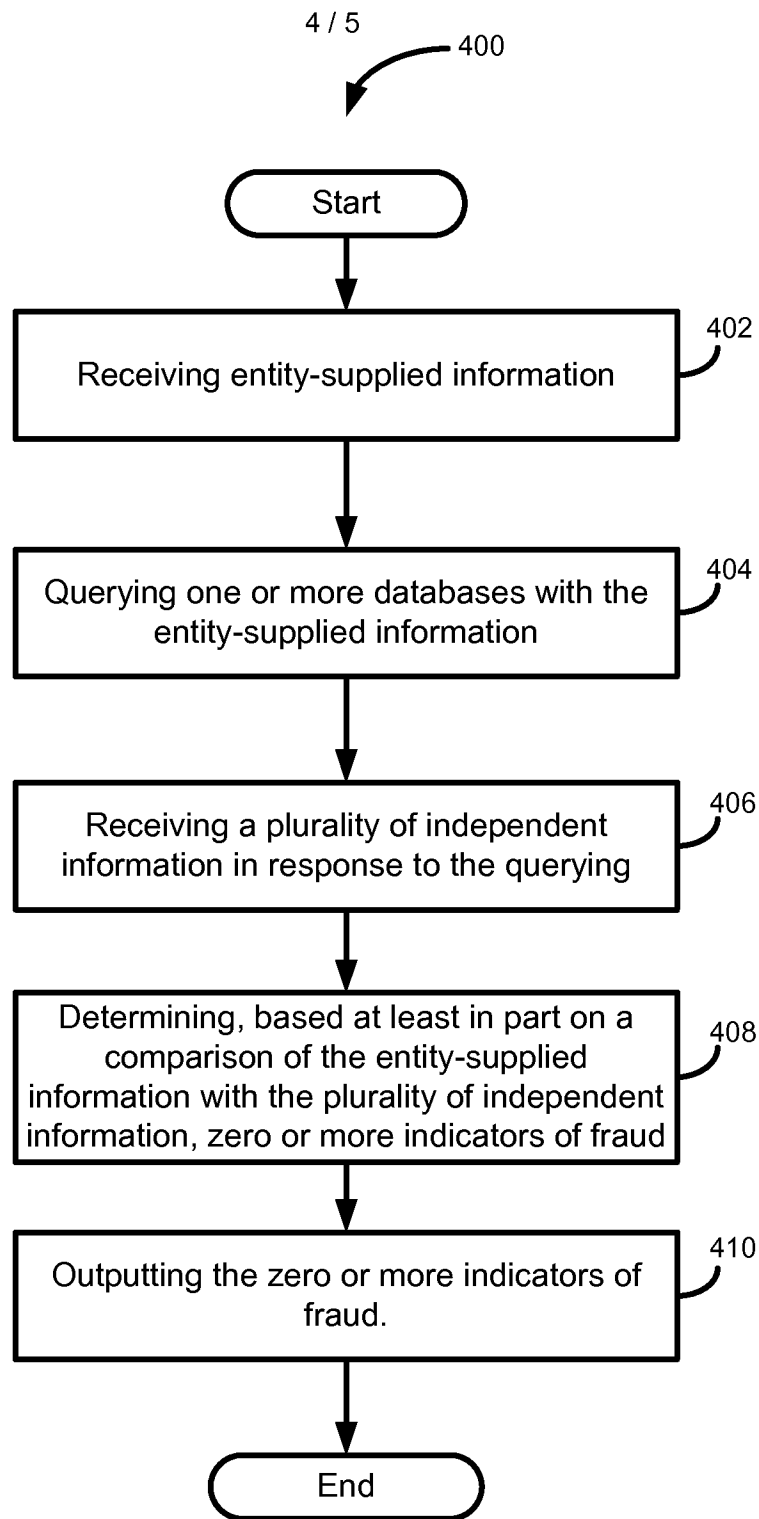


FIG. 4

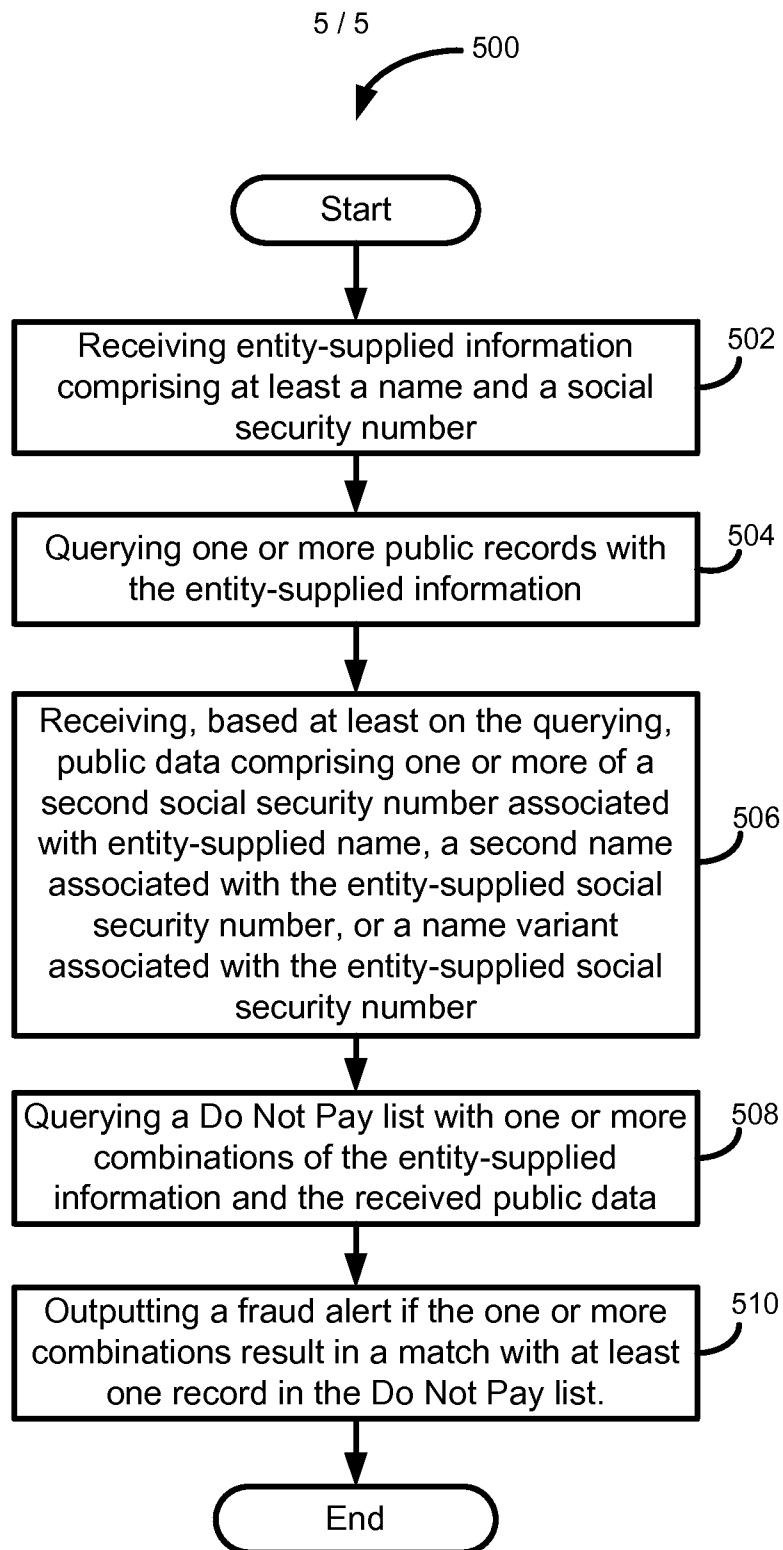


FIG. 5