(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 May 2002 (02.05.2002)

PCT

(10) International Publication Number
WO 02/35480 A1

(51) International Patent Classification[7]: G07C 9/00

(21) International Application Number: PCT/US01/00677

(22) International Filing Date: 1 February 2001 (01.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/695,407 25 October 2000 (25.10.2000) US

(71) Applicant: CATALINA MARKETING INTERNATIONAL, INC. [US/US]; 200 Carillon Parkway, St. Petersburg, FL 33716 (US).

(72) Inventor: HALAK, John, J.; 6717 Ashley Court, Sarasota, FL 34241 (US).

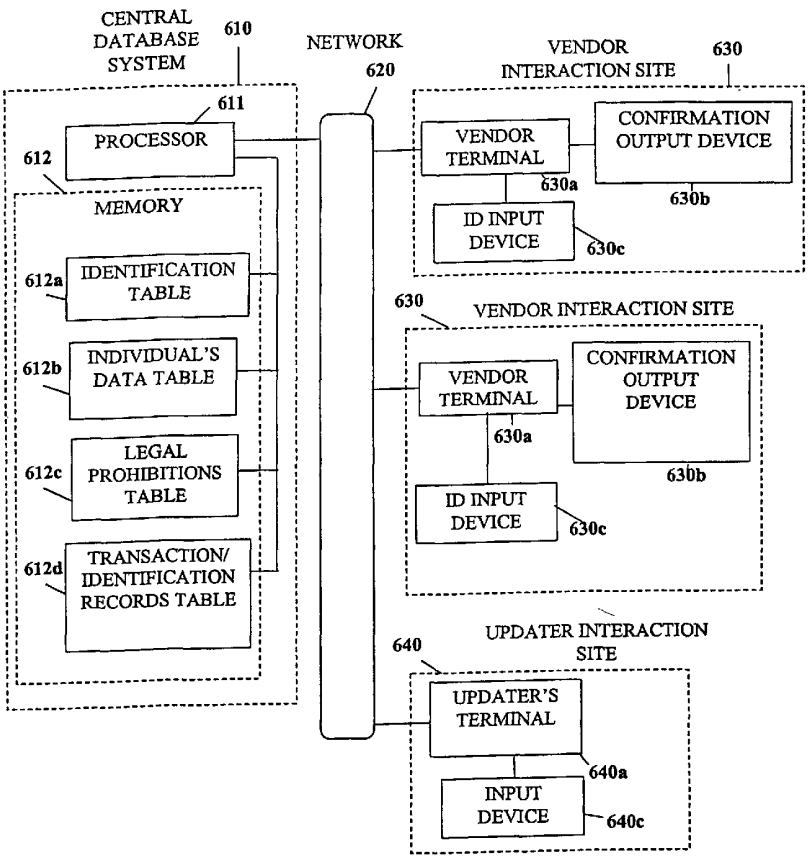
(74) Agent: NEIFELD, Richard, A.; Oblon, Spivak, McClelland, Maier & Neustadt, P.C., Crystal Square Five, 4th floor, 1755 Jefferson Davis Highway, Arlington, VA 22202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: METHOD AND SYSTEM USING BIOMETRICS TO DETERMINE WHETHER ONE IS AUTHORIZED TO MAKE A PURCHASE




(57) Abstract: A method, system, and computer-readable medium that determine and/or confirm whether an individual is legally entitle and/or permitted to purchase a restricted product based upon a biometric measurement. Biometric information is received and used to identify a group to which a potential customer belongs. This group membership information is used to confirm whether or not the individual is legally entitle and/or permitted to purchase a restricted product. This can be done, e.g., by comparing the determined membership information with jurisdictional information specific to a certain restricted product. Moreover, a record of the provided biometric information can be stored to reduce the liability of the vendor in the case of falsified information.

WO 02/35480 A1

**Published:**
— *with international search report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# Method and System Using Biometrics to Determine Whether One Is Authorized to Make a Purchase

## BACKGROUND OF THE INVENTION

### Field of the Invention:

This invention is directed towards determining and/or confirming whether an individual is legally entitled and/or permitted to purchase a restricted product based upon a biometric measurement. More specifically, this invention is directed to providing a vendor of consumer products and/or services immediate and definite confirmation that an individual who is attempting to make a purchase is or is not legally authorized to make the purchase.

### Discussion of the Background:

For any of a number of different reasons, many societies limit the ability of certain groups to purchase certain products. FIG. 1 provides an exemplary list of products and groups that are restricted from purchasing those products, as well as examples of grounds that are usually cited when justifying the restrictions placed upon those products.

For example, the purchase of firearms is proscribed in many jurisdictions by the group denoted as "criminals." The definition of "criminal" depends upon the jurisdiction in which the purchase is being made, and ranges from, e.g., convicted felons to unlicensed individuals. Regardless of the relevant definition of "criminal," several societies (i.e, countries, states, and/or other jurisdictional entities) feel that a prohibition on purchases of firearms by "criminals" is justified. These grounds include, but are not limited to, the desire to protect other members of society from unsafe operation of the restricted firearms by "criminals." The grounds for the restriction of other products include, e.g., preventing the members of the prohibited group from doing mental, physical, emotional, and/or moral harm to themselves and/or others and limiting the liability of the greater society to accomodate such mental, physical, emotional, and/or moral harm caused by members of the prohibited group either to themselves or to others.

Despite the broad acceptance of the desirability of prohibitions of purchases of certain products by prohibited groups, individual members of these groups often succeed at circumventing the prohibitions on their purchases. For example, there were about 10 million

drinkers in the United States of America were under age 21 in 1995 despite a country-wide prohibition on alcohol possession and purchases by those under 21 (attributed to SAMHSA, 1996 by the website "http://www.madd.org/stats/stat_youth.shtml" as of October 12, 2000, the contents of which are incorporated herein by reference). One method for circumventing the prohibitions on purchases involves falsification of legal documents so that these documents indicate that the individual is not a member of the prohibited group, such as, e.g., falsification, theft, and/or borrowing of identity documents. Another method for circumventing the prohibitions on purchases involves reliance upon a lack of diligence on the part of those making the sale, such as, e.g., purchasing cigarettes from a vending machine or purchasing seating for emergency exit rows on airlines as a minor over the Internet. It is clear that a more convenient and reliable method and system for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product is needed.

These simple prohibitions of the sale of certain products to select groups are enervated by the fact that the vendor is responsible for verifying the identity of the individual making the purchase. A natural conflict of interest thus exists between the vendor who profits individually from the sale of a product but yet is responsible for protecting society's interests in the transaction. For example, a server in a restaurant who stands to receive a large tip by providing a high markup bottle of wine to young drinkers may not be very diligent about confirming whether the young drinkers are legally entitled and/or permitted to purchase alcohol. A need thus exists to have separate entities representing the interests of both society and the vendor who wishes to profit.

Another problem with current methods and systems for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product is the lack of a uniform standard to which vendors can be held. For example, there is no clear standard for establishing when a "reasonable vendor" should have recognized falsified identity documents, especially in light of the broad range and quality of identity documents available for falsification. Thus, any showing of falsified identity documents by the purchaser can often reduce the perceived and/or real liability of a vendor who allows a transaction involving the restricted product and prohibited individual to proceed. Once again, this helps avert enforcement of societal prohibitions on purchases by certain groups.

## SUMMARY OF THE INVENTION

Accordingly, one object of this invention is to provide a novel method, system, and computer-readable medium for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product.

Another object of this invention is to provide a novel method, system, and computer-readable medium for providing a vendor of consumer products and/or services immediate and definite confirmation that an individual who is attempting to make a purchase is or is not legally authorized to make the purchase.

A further object of this invention is to provide a novel method, system, and computer-readable medium for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product that is more convenient and reliable than current methods and systems.

Still another object of this invention is to provide a novel method, system, and computer-readable medium that provides, according to one embodiment, separate entities, representing the interests of society and the vendor, for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product.

Yet another object of this invention is to provide a novel method, system, and computer-readable medium that allow, according to one embodiment, the establishment of a uniform "reasonable vendor" standard for the effort needed to confirm the group status of a potential customer.

In addition to the objects cited above, it is also an object of this invention to ensure that the objectives behind each legal restriction on entitlement to purchase a product, including the products and objectives described in FIG. 1, are met in a more effective manner.

These and other objects of the invention are realized by providing a novel method, system, and computer-readable medium that confirm whether an individual is legally entitled and/or permitted to purchase a restricted product. In some embodiments, this system, method, and computer-readable medium can be conveniently disposed and/or implemented to provide reliable conformation of an individual's entitlement to purchase a restricted product. In other embodiments, this system, method, and computer-readable medium can be operated by a party other than the vendor, thereby providing another representative of society's

interests. In some embodiments, this system, method, and computer-readable medium can be used to establish legal standards for the effort needed to confirm entitlement to purchase a restricted product. In other embodiments, this system, method, and computer-readable medium can be used to meet the objectives behind the prohibitions on purchases on restricted products. For example, embodiments of this system, method, and computer-readable medium can be used to more effectively lower the cost of auto insurance, minimize the incidence of lung cancer, prevent shootings in schools, reduce crime, delay the appearance of antibiotic-resistant bacteria, ensure the safe operation of emergency exits on airplanes, prevent children from gambling, protect the moral fiber of society's youth, prevent biological weapons attacks by terrorist groups, and hinder the fabrication of narcotics in drug labs, each of these objective corresponding to the exemplary restricted products described in FIG. 1. Each of these objectives can be more effectively met by addressing the difficulties unique to enforcement of each individual prohibition, such as, e.g., making the falsification of identity "documents" (i.e., biometric information) more difficult, automating confirmation for unattended restricted product distribution (e.g., vending machines), reducing the burden of confirming authorization to purchase at gun shows, making remote (e.g., telephonic and/or Internet) confirmation of identity possible, and reducing the burden of confirmation of professional licences that enable an individual to make certain purchases.

As used herein, the term "restricted product" refers to any product where the sale of that product to a group is prohibited by law. As such, it does not include simple confirmation of an individual's identity to, i.e., provide access to restricted facilities, financial accounts, or other "secure" places and/or information. Rather, a sales transaction involving a product must occur.

As used herein, the term "right" refers to a legal right or a private right to purchase a product. An example of a legal right is a legal authorization to, e.g., purchase alcohol. An example of a private right is a private authorization to, e.g., purchase admission to an amusement park ride.

## BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same become better understood by reference to the

following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. 1 illustrates in tabular format several restricted products, groups prohibited from purchasing those products, and commonly cited benefits of those restrictions;

FIG. 2 illustrates an exemplary network structure for confirming whether an individual is entitled and/or permitted to purchase a restricted product based upon a biometric measurement;

FIG. 3a and 3b illustrate two exemplary data records for storing an individual's biometric identification data and data regarding an individual;

FIGS. 4a and 4b illustrate two exemplary data records for storing data regarding the prohibitions within a certain jurisdiction and data regarding a particular transaction;

FIG. 5 is a flowchart illustrating one exemplary embodiment of a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product according to the present invention;

FIG. 6 is a flowchart illustrating another exemplary embodiment of a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product according to the present invention;

FIG. 7 is a flowchart illustrating yet another exemplary embodiment of a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product according to the present invention; and

FIG. 8 illustrates an exemplary computer system that can form several different units in an embodiment of the present invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views, and more particularly to FIG. 1 thereof, which provides illustrative examples of products and groups that presently have limited purchasing rights in the United States of America. Naturally, the present invention can be extended to other countries and adapted for applicable state and local regulations, as well as changes in laws and norms. Also included in FIG. 1 are examples of commonly-cited benefits behind limiting purchasing rights. For example, there are several objectives in the

USA behind the restriction of alcohol purchases by individuals under the age of 21. One of these objectives is to protect the restricted group from the product, since underaged individuals are widely perceived as unable to control their alcohol consumption. Another objective often cited is to prevent the operation of automobiles by individuals under the age of 21 who are legally intoxicated. Yet another objective is to limit the liability of society to provide for the welfare (e.g., the mental, emotional, financial, and physical health) of those in the restricted group. In other words, the purchase of alcohol by underaged individuals is perceived to lead to increased rates of alcoholism, property damage, other health damage, and even moral damage to and by the restricted group for which society is in part liable.

FIG. 2 illustrates an exemplary network structure for confirming whether an individual is legally entitled and/or permitted to purchase a restricted product based upon a biometric measurement. This network structure will include at least one vendor interaction site **630** that is connected by way of a network **620** to a central database system **610**. In alternate embodiments, network **620** can be dispensed with in whole or in part, and interaction site **630** can include the data and functionality herein attributed to the central database system **610**. Thus, the network **620** can be implemented either as a communications or telecommunications network, or as an electrical lead, wire, or bus within a computer. Moreover, central database system **610** can be divided into a plurality of database systems, each directed to a subset of the data and functionality ascribed to the central database system **610** illustrated in FIG. 2. Furthermore, some embodiments of the network structure may include an updater interaction site **640** from which the information stored in various table can be updated. As illustrated in FIG. 2, this updater interaction site **640** is connected to the central database system by way of network **620**. This is not necessarily the case, and the updater interaction site **640** and the central database system **610** can be combined into one or more physically discrete units. The updater interaction site **640** allows, e.g., physicians to update prescription information for a patient, law enforcement officials to enter felony convictions, and new biometric identification information to be entered as it becomes available.

The processor **611** of central database system **610** is used for coding and decoding data transmitted over network **620**, controlling reading and writing of data in tables **612a-d**, and analyzing the data in tables **612a-d**. The processor **611** can be any processor configured

for high volume data transmission and performing a significant number of mathematical calculations in processing communications (possibly as a webserver), database searches, and computational algorithms. A conventional personal computer or workstation with sufficient memory and processing capability may be configured to act as processor **611**. A PENTIUM III microprocessor such as the 1GHz PENTIUM III for the SC 242 manufactured by Intel Inc., a Motorola 500 MHZ POWERPC G4 processor, and the Advanced Micro Devices 1 GHz AMD ATHLON processor may all be used as the processor **611**. The tables **612a-d** may reside or be stored on any suitable processor-accessible data medium, including but not limited to any type of disk including floppy disks, optical disks, CD-Rom, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, flash memory, magnetic or optical cards, or any type of media suitable for storing electronic data.

The network **620** may be a local area network, a wide area network (such as the Internet), a virtual private network, and/or a connection via a public switched telephone network. In an exemplary embodiment, the network **620** includes a number of connection modalities, including a cable-modem connection, a DSL connection, a dial-up modem connection, and/or other suitable connection mechanisms.

The first type of interaction site, vendor interaction site **630**, includes a vendor terminal **630a** that would be located at, in an exemplary embodiment, the check-out counter of a store, a vending machine, a central location shared by several stores, a government-operated outlet (e.g., an alcoholic beverage commission (ABC) store), a mobile kiosk at a central location in a gun show, flea market, or street fair, an airline counter, an entrance of a nightclub, casino, or movie theater, a restaurant, a telephone where sales orders are placed, a pick-up counter at a pharmacy, or even an individual's home computer in the case of Internet transactions. The vendor interaction site **630** can include a processor similar to processor **611**, but in an exemplary embodiment it is simply dedicated to the reception and transmission of data over network **620** and the coding and decoding of data received from ID input device **630c** and output to confirmation output device **630b**.

Vendor interaction site **630** is designed to be operated by the vendor and/or the potential customer. Placement of the vendor interaction site **630** at a position where the vendor can control the operation of the device (e.g., check-out site, entrance to club or theater, prescription pick-up site) is preferred in order to avert falsification of identification

data received at ID input device **630c**. However, in certain transactions, such as in the case of Internet transactions or transactions at trade shows/flea markets, a vendor interaction site **630** that is physically removed from the vendor may be necessary because of constraints in time and money. Some locations of the vendor interaction site **630**, such as at a telephone where sales orders are placed, are intermediate between these two extremes, since the vendor interaction site **630** is at the vendor, but the prospective purchaser of the restricted product is distant and input identity information telephonically.

In some embodiments, vendor interaction site **630** can include a transaction input device (not shown) such as a keyboard, touch screen, computer mouse, bar code reader, magnetic reader (including strip, disk, and tape reader), smart card reader, pressure sensor, motion detector, electromagnetic receiver, voltmeter, heat sensor, and other transducer capable of receiving transaction identification information. The transaction identification information will allow the vendor and/or potential customer to identify the product(s) and/or jurisdiction of the potential transaction to the vendor terminal **630a** so that this information may be transmitted to processor **611** for use when confirming that an individual is legally entitled and/or permitted to purchase a restricted product. Alternatively, as mentioned above, if the data storage table **612c** and processor **611** is located at the vendor interaction site, the transaction (e.g., product and jurisdictional) information need not be transmitted over network **620** to central database system **610**. Alternatively, the transaction (e.g., product and jurisdictional) information need not be input with every transaction, but rather can be set during installation of the system. For example, a vendor interaction site operated by an airline can always indicate that the product is an airline ticket, and a vendor interaction site operated by an alcohol beverage control store can always indicate that the product is alcohol and the jurisdiction is the local state.

Each of the vendor interaction sites **630** include an ID input device **630c** that receives biometric identifying information from a potential customer and forwards that information to a processor **611** where it is compared with identification table **612a** to provide a confirmed identification of the prospective customer. ID input device **630c** can be any of a number of recognition devices that receive and/or generate identifying information regarding a potential customer. Examples of embodiments of ID input device **630c** that generate identifying information include voice transduction devices (e.g., microphones), digital cameras,

fingerprint readers, iris recognition devices, genetic identification devices, pressure sensors, motion detectors, electromagnetic receivers, voltmeters, heat sensors, and other transducers capable of measuring or receiving measurement information regarding one or more biometric property of an individual, and transferring this information to a digital processor. Examples of embodiments of ID input device **630c** that receive identifying information include processors configured to receive digitized image, sound, pattern, genetic, and/or other information and analog-to-digital converters configured to convert analog image, sound, pattern, and/or genetic information into a digital format. Thus, the ID input device **630c** of the vendor interaction site **630** need not conduct the actual transduction of the biometric parameter, but rather ID input device **630c** must simply be capable of receiving biometric identification input from a potential customer.

The ID input device **630c** is biometric. In other words, the ID input device **630c** uses biological information and/or parameters to identify the potential customer. One significant advantage of this approach includes the fact that biological information is difficult for a person to falsify. This adds yet another layer of security to the identification process. Furthermore, the parameters measured in biometric identification are generally universal to all humans. For example, even though an individual from a country foreign to the vendor may possess unfamiliar, and therefore easier to forge, identification documents, the biological parameters used to identify an individual are relatively universal to all humans and therefore more reliable confirmation of an individual's ability to purchase can be obtained. Moreover, since the biological parameters are relatively universal to all humans, uniform legal standards of accountability can be established. For example, the use of a test that confirms that an individual is legally entitled and/or permitted to purchase a restricted product with a false positive (indicating that an individual is permitted to purchase when, in fact, the individual is not permitted to purchase) rate below 0.1% may be established in a jurisdiction as a reasonable standard for a vendor to meet to free the vendor from liability for the transaction. Finally, since the vendor interaction site **630** (including the ID input device **630c**) and/or the central database system **610** can be operated by a third party, the conflict of interest that arises between a vendor's desire to make a sale and the vendor's need to enforce societal laws need not arise.

Suitable types of biometric identification include photographic facial feature

recognizers, fingerprint readers, voice and iris recognition devices, and genetic identification devices including gene chips. Facial feature recognizers are described in U.S. Patent No. 6,072,894, the contents of which are incorporated herein by reference. Fingerprint readers are described in, for example, U.S. patent Nos. 5,469,506, 4,747,147, 5,109,427, 3,882,462, 5,631,971, the contents of all of which are incorporated herein by reference. Briefly in regard to fingerprint readers, a scanner as ID input device **630c** creates a digital image of a fingerprint by transducing the pattern of light reflected from a fingertip. Alternatively, ID input device **630c** can be formed by a processor configured to, e.g., receive scanned fingerprint information from a remote scanner, such as an individual's home scanner in the case of an Internet transaction. A processor **611** using Fingerprint Identification (FID) software can be used to analyze the pattern of reflected light by searching for two types of specific features. One feature is the core, or center of the print. The other features are minutia -- points at which ridges end or divide. The processor **611** thus describes a series of vectors relating the minutia. Even if a finger is off-center or rotated during the scan, the vectors describing the relationships between the minutia do not significantly change and are complex enough to be unique. Ridges and minutia are used to perform one of two possible identifications, one-to-one or one-to-many. A one-to-one search occurs in an identity verification system (IVS), which is used for security purposes. The IVS knows in advance who a potential customer claims to be, and compares the pattern of minutia of a fingerprint patterned freshly scanned (or received) at ID input device **630c** and transmitted from vendor terminal **630a** to processor **611** with a known record of the fingerprint stored in the central database system **610** identification table **612a**. Because not all minutia may be captured due to a cut or other aberration, the best the processor **611** can do is determine a probability that the print matches some other fingerprint in identification table **612a**. When a known print

core to the rim of the print. Although counting ridges is quick, it is inherently inaccurate. The number of ridges on the same finger can easily change from print to print, depending on how hard the finger is pressed against the scanner. Also, the range of ridges on all fingers is not that varied and usually yields a count between 10 and 20. However, ridge counting still eliminates obvious mismatches. The processor **611** then examines the possible matches generated by ridge counting, looking for further similarities in the pattern of minutia.

Voice recognition is described in U.S. patent Nos. 6,640,490, 5,751,904, and 5,745,64, the contents of which are hereby incorporated by reference. Briefly, voice recognition software controlling a processor **611** must first go through an enrollment of candidate voices that are to be recognized by the software and store this enrollment information in an identification table **612a**. In order to add his or her voice to the list of candidate voices, a person must dictate a known text for a suitable time, commonly 10 minutes to an hour. From this sampling, the software creates a table of vocal references for many individuals in an identification table **612a**, which are the ways in which the speaker's pronunciation of phonemes varies from models of speech. After enrollment, the speaker can later dictate the text he or she wants the software to compare with the vocal references of the candidate voices into a microphone acting as ID input device **630c**, preferably one that uses noise-cancellation to eliminate background sounds. Alternatively, a processor and/or A/D converter can act as ID input device **630c** and receive digitized voice information from a remote microphone. The quality of the microphone acting as ID input device **630c** (or supplying identification information to ID input device **630c**) and power of the computer processor **611** are relevant to the quality of voice recognition. The signal generated by a microphone acting as ID input device **630c** can be sampled at rates commonly above 30 kHz but preferably above 50 kHz by an analog-to-digital converter (ADC) in vendor terminal **630a** and converted using pattern recognition algorithms to a set of measurements of several factors, including pitch, volume, frequency, length of phonemes, and silences. The measurements can be compressed for quicker processing, and the software's speech engine makes adjustments to the measurements by factoring in, for example, background sounds and the acoustic characteristics of the microphone. The acoustic recognizer such as a neural network algorithm controlling processor **611** compares the corrected measurements from vendor terminal **630a** to a database of previous measurements associated with the candidate

individuals, compiled by previously sampling the speech of those individuals and stored in identification data table **612a**. For each measurement, such as pitch, the recognizer finds the database entries in identification table **612a** that most closely match that specific measurement. To narrow the selection further, the engine compares another measurement, to the measurement of only those database entries in identification table **612a** that received a high score on the exemplary pitch measurement. The process continues until the processor **611** finds the candidate voice that most closely matches the sample voice across the entire range of measurements.

An alternate embodiment of ID input device **630c** relies upon DNA fingerprinting tests to covertly identify the potential customer. DNA fingerprinting tests are based on the genetic differences that exist between individuals, and are described in the article entitled "Automation of DNA Fingerprinting: a Multi-Color Fluorophore Approach" published by Applied Biosystems. Other exemplary approaches in those described in U.S. patent Nos. 5,831,065, 5,576,180, 4,880,750, and 6,077,668, the contents of all of which are hereby incorporated by reference. Briefly, according to embodiment, currently, the most informative genetic markers for characterization of humans are the variable number of tandem repeat (VNTR) loci. VNTR alleles differ in size by the number of tandem repeat sequences. DNA can be isolated from blood or other cell or tissue samples and the DNA sequences of VNTR loci can be specifically amplified by PCR. When PCR with automated DNA purification, automated primer synthesis, and automated fluorescent fragment analysis are performed at an ID input device **630c** (or the data resulting transmitted from other instruments to an ID input device **630c**), individuals can be biometrically identified. These procedures have been automated using commercially available equipment, namely the GENEPURE 341 Nucleic Acid Purification System, the PCR-MATE 391 DNA Synthesizer, and the GENE SCANNER 362 Fluorescent Fragment Analyzer available from Applied Biosystems.

Briefly describing these steps, DNA can purified using the Applied Biosystems GENEPURE 341 Nucleic Acid Purification System. This instrument is used for the automated purification of nucleic acid from a broad range of sample types. A protocol specifically designed for handling small quantities of DNA on the GENEPURE system makes use of the system's phenol-chloroform chemistry and BASEBINDER resin. Whole

blood samples (50 µL) can be diluted to 1.5 mL with Tris-buffered saline (TBS) and loaded directly into a GENEPURE reaction vessel containing 2X Lysis Buffer that had been previously delivered by the GENEPURE system and heated to 60°C. The system can next deliver Proteinase K and perform a one-hour digestion while shaking. Then the system can perform two extractions with a phenol/water/chloroform reagent and one extraction with chloroform. The BASEBINDER resin can be added to each reaction vessel and the system used to deliver sodium acetate and isopropanol. Under these conditions, the genomic DNA binds to the resin. The system can collect the resin/precipitate complex on a PRECIPITATE II filter and rinse it with ethanol to remove any trace contaminants. The DNA can then be eluted from the resin with water.

Prior to the purification, oligonucleotide primers specific for three VNTR target loci can be synthesized on a PCR-MATE 391 DNA Synthesizer using fast oligonucleotide deprotecting (FOD) phosphoramidites and the standard 0.2 µmol scale synthesis cycle. Common target VNTR loci are Apo B (1), pMCT118 (2), and pNZ22 (3). To permit the attachment of a fluorescent dye, an AMINOLINK 2 amine linker can be added to the 5' end of each of the primers during the last monomer addition using the standard synthesis cycle. After cleavage and deprotection of the oligonucleotides, a fluorescent dye-NHS ester can be coupled to the primers to be labeled through the AMINOLINK 2 moiety.

DNA samples can be amplified at the VNTR low using the GENEAMP PCR DNA Amplification System from Perkin-Elmer Cetus Instruments and the fluorescence-labeled oligonucleotide primers. The primers were designed with a different dye label for *in situ* labeling of PCR products as follows: Apo B (FAM-blue), pMCT118 (JOE-green), and pYNZ22 (TAMRA-yellow).

Aliquots of the fluorescence-labeled PCR products can be combined with an internal-lane size standard, GENESCAN-1000, labeled with the "red" fluorophore, ROX. Samples can then be loaded into a 2% agarose gel on a GENE SCANNER and electrophoresed through a 4-cm "well-to-read region" at 4 volts/cm.

The GENE SCANNER system uses multi-color, fluorescent based DNA sequencing technology for submarine agarose gel electrophoresis. The system incorporates a multi-line argon ion laser, which scans across the gel to excite fluorescence from passing dye-labeled PCR products. The emitted light is filtered collected, and transferred as digital signals, which

are automatically analyzed by a computer to assign fragment lengths and quantify fluorescence. Thereafter, the measured fluorescent patten is compared with previously measured fluorescent patterns in identification table **612a** corresponding to a number of candidate individuals. This continues until a matching pattern associated with a specific individual is located.

Regardless of the nature of ID input device **630c**, once identification data is produced and/or digitized, it can be transferred from vendor terminal **630a** to processor **611** of central database system **610**. Naturally, this can be done by way of a network **620**, or alternatively a processor similar to processor **611** can be part of vendor interaction site **630** (not shown). Nevertheless, the identification data is relayed to processor **611**, where it is compared to tables stored in identification data storage records **612a**. An exemplary data structure for identification table **612a** is illustrated as Data Record A **710** of FIG. 3a.

Upon identification of a matching or near-matching record, the processor **611** further accesses tables **612b** , **612c**, and **612d**. Individual data storage table **612b** contains data regarding the individual potential customer such as, for example, the age of the individual, a criminal record, a psychological profile, a record of professional licenses, a record of prescribed medications, a record of other licenses such as material handling licenses or firearm licenses, or information relating to membership in any other group that is prohibited from purchasing one or more products. An exemplary data structure of a record included therein is illustrated in FIG. 3b. Once processor **611** identifies the potential customer, the potential customer's data record in individual table **612b** is accessed by processor **611** to confirm whether an individual is legally entitled and/or permitted to purchase a restricted product.

The confirmation of whether an individual is legally entitled and/or permitted to purchase a restricted product can be done in light of information stored in a legal prohibition table **612c**. Legal prohibition table **612c** can include several jurisdictional records of the identifying characteristics of groups that are prohibited from making certain purchases. An exemplary data structure of a record included therein is illustrated in FIG. 4a. By comparing the individual consumer data obtained from individual consumer table **612b** with legal prohibitions obtained from legal prohibition table **612c** in light of the jurisdiction of the vendor at vendor interaction site **630**, the processor **611** can confirming whether a potential

customer is legally entitled and/or permitted to purchase a restricted product based upon a biometric measurement received at ID input device **630c**. This confirmation can be relayed to vendor interaction site **630** so that the vendor may complete the transaction.

In order to provide documentation for the authorities in case a proscribed transaction inadvertently occurs, central database system **610** includes, in some embodiments, a data warehousing capability. Transaction/identification records table **612d** can store both the nature of the potential transaction, and the identifying information provided by the potential customer. An exemplary data structure of a record included in an exemplary transaction/identification records table **612d** is illustrated in FIG. 4b. As mentioned before, the data warehousing of transaction/identification records table **612d** need not be included in central database system **610**, but can instead form a separate database system (not shown).

The confirmation that an individual is legally entitled and/or permitted to purchase a restricted product is returned to vendor terminal **630a**, upon which the confirmation is output using confirmation output device **630b**. Confirmation output device **630b** likewise can be made of any of a number of different devices, including a computer monitor, printers (paper or otherwise), magnetic writing devices (including disk drives, magnetic strip writers, tape writers), bar code writers, television screens, radio broadcast, Internet data transmission, print advertisement in a newspaper or newsletter, or simply electronic confirmations communicated automatically to another device, such as, for example, a check-out register, a booking software, a vending machine, an order-placement system, and/or a prescription medicine dispenser.

FIG. 3a and 3b illustrate two different data record structures **710** and **720** that may be used to store an individual's biometric identification data and data regarding an individual in data storage tables **612a** and **612c** of FIG. 2. Biometric identification factors **710d**, **710e**, and **710f** are compared with the same biometric parameters measured at ID input device **630c**. Once a suitable match or near-match is found, the associated potential customer's name (or other identifying info) **710c** is drawn from the record **710**, and used to search data storage tables **612c** until an individual data record **720** with a matching potential customer's name field **720c** is found. Individual information **720d**, **720e**, **720f**, and **720g** is used to identify groups to which the potential customer belongs that may be prohibited from making certain purchases.

FIGS. 4a and 4b illustrates two different data record structures **730** and **740** that may be used to store data regarding the prohibitions within a certain jurisdiction **730c** and data regarding a particular transaction within a particular jurisdiction in tables **612b** and **612d** of FIG. 2, respectively. The jurisdiction name (or other identifying info) **730c** can be matched to jurisdictional information input or stored at vendor interaction site **630**. Information regarding transactions involving restricted products can be stored in fields **730d**, **730e**, **730f**, **730g**, and **730h**. This information may include, e.g., an age group that is prohibited from purchasing a product, licensing requirements for a restricted product, "criminal" record requirements, or the time of year in which a certain product may be purchased. This is used in conjunction with the information available regarding individual potential customer in data record B **720** to confirm whether an individual potential customer is or is not legally authorized to make a purchase. Namely, restricted product information identified at the vendor interaction site **630** is used to select a restriction information field **730d-h** in a data record C **720** selected by comparing the jurisdiction name **730c** with jurisdiction information provided at vendor interaction site **630**. The restriction information from one or more restriction information fields **730d-h** is compared with the individual information **720d-g** selected using a potential customer's name **720c** identified using one or more of the biometric identification factors **710d-f**. The comparison between the restriction information from one or more restriction information fields **730d-h** and the individual information **720d-g** is used to confirm whether an individual potential customer is or is not legally authorized to make a purchase. For example, if the restriction information from one or more restriction information fields **730d-h** indicates that the admission of individuals under the age of 17 to a particular movie in a particular jurisdiction is prohibited and the individual information **720d-g** indicates that the potential customer is only 2 years old, than a confirmation that the potential customer is not legally entitled to purchase the admission to the particular movie will be returned to the vendor interaction site **630**.

FIG. 5 is a flowchart illustrating a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product according to one embodiment of the present invention. This method can be performed in whole or in part by a third party (i.e., neither the vendor nor the potential customer), removing the vendor's conflict of interest in confirming a potential customer's eligibility to make a purchase. In step **5100**, biometric

identification is received from a potential customer. As described in regard to identification input device **630c** of FIG. 2, the reception of biometric information can include the transduction of one or more biological parameters of the potential customer, or simple reception of data related to one or more biological parameters. According to one embodiment, the other identification information, such as the potential customer's name, is received. In this case, the customer's name can be used to assist in locating the supposedly relevant identification record **710** in identification table **612a** of central database system **610**, and a simple comparison between previously recorded biometric identification factors **710d-f** and the newly received (in step **5100**) biometric identification factors can occur. The reception of biometric identification factors in step **5100** can occur in a public facility such as a checkout cashier of a store, over a telephone line, or over a network connection.

In step **5200**, the group membership of the potential customer can be identified based upon previously determined identification information regarding the potential customer. These group memberships can be related to the age (e.g., a specific age or class of ages such as "older than 21," mental history, criminal records, medical record, prescription information, professional licenses, and/or other licenses held by the individual. According to one embodiment, the group membership of the individual is determined only in light of jurisdictionally applicable restrictions on products. For example, in 1999 a twenty-year old in the United States of America would belong to a group that is prohibited from purchasing alcohol, whereas that same twenty-year old in Germany would belong to a group that was not prohibited from purchasing alcohol. The determination of group membership can be performed in light of transaction information provided by the vendor interaction site **630**.

Once the group membership of the potential customer has been identified, this group membership is compared with the applicable jurisdictional restrictions on purchases of one or more products. These jurisdictional restrictions can be stored, e.g., in data record **730** in legal prohibitions table **612c** of central database system **610** or in similar data record at the vendor interaction site **630**. Alternatively, step **5300** can be performed manually by a vendor based upon the group membership information identified in step **5200**.

Once a comparison between the identified group membership of the potential customer and the applicable jurisdictional restrictions on purchases has been performed, whether or not the potential customer has the right to purchase a restricted product is

confirmed in step **5400**. This confirmation can take the form of a simple yes/no indication, the activation of another device such as a cash register or a vending machine, and/or the display of one or more group memberships of the individual. For example, if the comparison between group memberships and the applicable jurisdictional restrictions is performed manually, step **5400** reduces to simple transmission of the identified group memberships to the vendor.

FIG. 6 is a flowchart illustrating a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product according to one embodiment of the present invention that includes a new step **6150** wherein transaction information is received from a vendor. This method can be performed in whole or in part by a third party (i.e., neither the vendor nor the potential customer), removing the vendor's conflict of interest in confirming a potential customer's eligibility to make a purchase. The new step **6150** can be performed automatically, for example by the processor **611** of FIG. 2 . The transaction information can be loaded by a vendor for every transaction involving a restricted product such as, e.g., every new prescription order placed, or this information can be stored at vendor interaction site **630** and transmitted along with received biometric information.

FIG. 6 also includes a step **6500** wherein a record of the transaction involving a restricted product is recorded in a data warehouse, such as the transaction/identification records table **612d** of central database system **610**. This may be used to limit the liability of a vendor by storing any falsified identification information. Alternatively, if a particular restricted product later finds its way into the hands of individuals belonging to a group that is prohibited from purchasing that product, then the police may have a starting point for tracking the flow of the restricted product. For example, if a certain lot of restricted chemicals is found in a narcotics production lab, the police may be able to trace the path of the lot of chemicals from the manufacturer/distributor through a legitimate buyer to the production lab. Alternatively, if an underage drinker is involved in an accident while driving under the influence of alcohol, the police may be able to identify a legitimate purchaser (i.e., an older sibling or a friend of the underage drinker) who transferred the restricted alcohol to the underage drinker.

FIG. 7 is a flowchart illustrating another exemplary embodiment of a method for confirming whether an individual is entitled and/or permitted to purchase a restricted product

according to the present invention. This method illustrates one form in which the current invention can be performed by a third party (i.e., neither the vendor nor the potential customer), removing the vendor's conflict of interest in confirming a potential customer's eligibility to make a purchase. As such, it represents a specific embodiment of portions of the process illustrated in FIG. 5. In step **7100**, biometric identification information is received. This information ultimately originates from the potential consumer, but it can be transduced and relayed by the vendor to the third party performing the confirmation. In this case, the ID input device **630c** comprises a communication interface configured to receive biometric identification information. In step **7200**, the received biometric identification information is matched to a known individual and his or her individual data. In step **7300**, the individual data regarding the known individual is simply relayed to a vendor, who may then be responsible for comparing this data with the relevant transaction (e.g., product and jurisdiction) information. In this case, the confirmation whether an individual is legally entitled and/or permitted to purchase a restricted product is just the individual data regarding the known individual.

FIG. 8 illustrates a computer system **801** that can form several different units in an embodiment of the present invention. For example, computer system **801** can alternately form the central database system **610**, a vendor interaction site **630**, or an updater interaction site **640** of FIG. 1. For this reason, the computer system **801** will be described using unique reference numerals. When a part of computer system **801** that is analogous to a part in another figure is described, this will be explicitly stated in the text. Computer system **801** includes a bus **802** or other communication mechanism for communicating information, and a processor **803** coupled with bus **802** for processing the information. Processor **803** can form processor **611** and/or one or more of the vendor terminals **630a** or updater terminal **640a** of FIG. 1. Computer system **801** also includes a main memory **804**, such as a random access memory (RAM) or other dynamic storage device (e.g., dynamic RAM (DRAM), static RAM (SRAM), synchronous DRAM (SDRAM), flash RAM), coupled to bus **802** for storing information and instructions to be executed by processor **803**. In addition, main memory **804** may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor **803**. Computer system **801** further includes a read only memory (ROM) **805** or other static storage device (e.g., programmable

ROM (PROM), erasable PROM (EPROM), and electrically erasable PROM (EEPROM)) coupled to bus **802** for storing static information and instructions for processor **803**. A storage device **807** and/or **808**, such as a magnetic disk or optical disk, is provided and coupled to bus **802** by way of a disk controller **806** for storing information and instructions. Storage device **807** and/or **808** can contain the tables **612a**, **612b**, **612c**, and **612d** of FIG. 1.

The computer system **801** may also include special purpose logic devices (e.g., application specific integrated circuits (ASICs)) or configurable logic devices (e.g., generic array of logic (GAL) or reprogrammable field programmable gate arrays (FPGAs)). Other removable media devices (e.g., a compact disc, a tape, and a removable magneto-optical media) or further fixed, high density media drives, may be added to the computer system **801** using an appropriate device bus (e.g., a small computer system interface (SCSI) bus, an enhanced integrated device electronics (IDE) bus, or an ultra-direct memory access (DMA) bus). Such removable media devices and fixed, high density media drives can also contain the tables **612a**, **612b**, **612c**, and **612d** of FIG. 1. The computer system **801** may additionally include a compact disc reader, a compact disc reader-writer unit, or a compact disc juke box, each of which may be connected to the same device bus or another device bus.

Computer system **801** may be coupled via bus **802** to a display **810**, such as a cathode ray tube (CRT), for displaying information to a computer user. Display **810** can form a confirmation output device **630b** of FIG. 1, especially when the confirmation is a yes/no indication that an individual is entitled to purchase a product. The display **810** may be controlled by a display or graphics card. The computer system includes input devices, such as a keyboard **811** and a pointing device **812** (e.g., a cursor control), for communicating information and command selections to processor **803**. The keyboard **811** and a pointing device **812** (e.g., a cursor control) can form an input device **640c** of an updater interaction site **640**. The pointing device **812** (e.g., cursor control), for example, is a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor **803** and for controlling cursor movement on the display **810**. In addition, a printer (not shown) may provide a confirmation output device **630b** of FIG. 1, especially wherein the confirmation is a ticket for admission to a mature content performance.

The computer system **801** performs a portion or all of the processing steps of the invention in response to processor **803** executing one or more sequences of one or more

instructions contained in a memory, such as the main hard disk memory **807**. Such instructions may be read into the main hard disk memory **807** from another computer readable medium, such as storage device **808**. One or more processors in a multi-processing arrangement may also be employed to execute the sequences of instructions contained in main hard disk memory **807**. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions. Thus, embodiments are not limited to any specific combination of hardware circuitry and software.

As stated above, the system **801** includes at least one computer readable medium or memory programmed according to the teachings of the invention and for storing data structures, tables, records, or other data described herein. Examples of computer readable media are compact discs, hard disks, floppy disks, tape, magneto-optical disks, PROMs (EPROM, EEPROM, Flash EPROM), DRAM, SRAM, SDRAM, etc. Stored on any one or on a combination of computer readable media, the present invention includes software for controlling the computer system **801**, for driving a device or devices for implementing the invention, and for enabling the computer system **801** to interact with a human user. Such software may include, but is not limited to, device drivers, operating systems, development tools, and applications software. Such computer readable media further includes the computer program product of the present invention for performing all or a portion (if processing is distributed) of the processing performed in implementing the invention.

The computer code devices of the present invention may be any interpreted or executable code mechanism, including but not limited to scripts, interpreters, dynamic link libraries, Java classes, and complete executable programs. Moreover, parts of the processing of the present invention may be distributed for better performance, reliability, and/or cost.

The term "computer readable medium" as used herein refers to any medium or media that participate in providing instructions to processor **803** for execution. A computer readable medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical, magnetic disks, and magneto-optical disks, such as storage device **807** and/or **808**. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus **802**. Transmission media also may also take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

Common forms of computer readable media include, for example, hard disks, floppy disks, tape, magneto-optical disks, PROMs (EPROM, EEPROM, Flash EPROM), DRAM, SRAM, SDRAM, or any other magnetic medium, compact disks (e.g., CD-ROM), or any other optical medium, punch cards, paper tape, or other physical medium with patterns of holes, a carrier wave (described below), or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying out one or more sequences of one or more instructions to processor **803** for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions for implementing all or a portion of the present invention remotely into a dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system **801** may receive the data on the telephone line and use an infrared transmitter to convert the data to an infrared signal. An infrared detector coupled to bus **802** can receive the data carried in the infrared signal and place the data on bus **802**. Bus **802** carries the data to main hard disk memory **807**, from which processor **803** retrieves and executes the instructions. The instructions received by main hard disk memory **807** may optionally be stored on a removable media storage device **808** either before or after execution by processor **803**.

Computer system **801** also includes a communication interface **813** coupled to bus **802**. As described previously, communication interface **813** can itself form a confirmation output device **630b** when an electronic confirmation is communicated electronically to another device such as a cash register, credit-card billing device, ticket printer, boarding pass printer, and/or vending machine. Such electronic confirmations can include, for example, electronic codes automatically transmitted to the register of a vendor, electronic order placed directly with a vendor upon the customer's indication, or deductions from a customer's account upon purchase or order of a product. Communication interface **813** provides a two-way data communication coupling to a communications network **816** that is connected to a local network **815**. For example, communication interface **813** may be a network interface card to attach to any packet switched local area network (LAN). As another example, communication interface **813** may be an asymmetrical digital subscriber line (ADSL) card, an integrated services digital network (ISDN) card or a modem to provide a data

communication connection to a corresponding type of telephone line. Wireless links may also be implemented. In any such implementation, communication interface **813** sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

Communications network **816** typically provides data communication through one or more networks to other data devices. For example, communications network **816** may provide a connection to another computer (not shown) through local network **815** (e.g., a LAN) or through equipment operated by a service provider, which provides communication services through a communications network **816**. Communications network **816** can form network **620** of FIG. 1. According to one embodiment, computer **801** is one of the interactions sites **630** while central database system **610** is formed by another computer **801**. In some embodiments, local network **815** and communications network **816** preferably use electrical, electromagnetic, or optical signals that carry digital data streams. The signals through the various networks and the signals on network link **814** and through communication interface **813**, which carry the digital data to and from computer system **801**, are exemplary forms of carrier waves transporting the information. Computer system **801** can transmit notifications and receive data, including program code, through the network(s), network link **814** and communication interface **813**.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

CLAIMS:

1. A method comprising the steps of:

receiving biometric identification information from a potential customer;

identifying a group membership of said potential customer; and

confirming to a vendor a right of said potential customer to purchase a product.

2. The method according to claim 1, wherein said product comprises alcohol.

3. The method according to claim 1, wherein said product comprises cigarettes.

4. The method according to claim 1, wherein said product comprises a firearm.

5. The method according to claim 1, wherein said product comprises a prescription medication.

6. The method according to claim 1, wherein said product comprises a casino admission.

7. The method according to claim 1, wherein said product comprises a mature content performance admission.

8. The method according to claim 1, wherein said product comprises a seat within an airplane.

9. The method according to claim 1, wherein said product comprises a pathogenic organism.

10. The method according to claim 1, wherein said product comprises a chemical.

11. The method according to claim 1, wherein said confirming step comprises transmitting individual information to a vendor.

12. The method according to claim 1, wherein said confirming step comprises transmitting a yes/no indication to a vendor.

13. The method according to claim 1, wherein said confirming step comprises transmitting a confirmation over a communications network to a vendor.

14. The method according to claim 1, wherein said identifying step comprises determining an age of said potential customer who provides said biometric identification information.

15. The method according to claim 1, wherein said identifying step comprises determining a license to purchase a product held by said potential customer who provides said biometric identification information.

16. The method according to claim 15, wherein said license is a professional license.

17. The method according to claim 1, wherein said receiving biometric identification information step comprises scanning a fingerprint of said potential customer.

18. The method according to claim 1, wherein said receiving biometric identification information step comprises receiving data related to a scan of a fingerprint of said potential customer.

19. The method according to claim 1, wherein said receiving biometric identification information step is performed under a vendor's supervision.

20. The method according to claim 1, wherein said receiving biometric identification information step is performed at a home of said potential customer.

21. The method according to claim 1, wherein said receiving biometric identification information step comprises recognizing a voice transmitted over a telephone line.

22. The method according to claim 1, further comprising comparing said group membership of said potential customer with a prohibited group prohibited from purchasing a product in a jurisdiction.

23. The method according to claim 22, wherein said comparing step comprises determining an age of said potential customer.

24. The method according to claim 22, further comprising receiving transaction information from a vendor, wherein said comparing step comprises accessing a list of restricted products for a jurisdiction.

25. The method according to claim 24, wherein said transaction information comprises a restricted product name and said jurisdiction of said vendor.

26. The method according to claim 1, further comprising a step of storing a record of a confirmed transaction.

27. The method according to claim 26, wherein said storing step comprises storing said biometric information, product information, and a jurisdiction of said vendor.

28. A system, comprising:

a biometric information receiver configured to receive biometric information from a potential customer;

a processor in communication with said biometric information receiver and configured to identify a group membership of said potential customer; and

a confirmation output device in communication with said processor and configured to provide a confirmation of whether said potential customer has a right to purchase a product .

29. The system according to claim 28, further comprising:

an identification record configured to store previously-loaded biometric information regarding an individual;

an individual's data record configured to store data regarding said individual,

wherein said processor compares said received biometric information to said previously loaded biometric information to identify said group membership of said potential customer using said individual's data record.

30. The system according to claim 28, further comprising:

a prohibitions record configured to store data regarding a legal prohibition of a purchase by a group.

31. The system according to claim 30, wherein said prohibitions record is located at a vendor.

32. The system according to claim 30, wherein said prohibitions record is located at a central database.

33. The system according to claim 28, wherein said biometric information receiver comprises a biometric information transducer.

34. The system according to claim 28, wherein said biometric information receiver comprises a data communications receiver.

35. The system according to claim 28, wherein said confirmation output device is configured to provide an age of said potential customer.

36. The system according to claim 28, wherein said confirmation output device is configured to provide a criminal record of said potential customer.

37. The system according to claim 28, wherein said confirmation output device is configured to provide a confirmation of a license of said potential customer.

38. The system according to claim 37, wherein said license is a professional license.

39. The system according to claim 28, wherein said confirmation output device comprises a ticket printer.

40. The system according to claim 28, wherein said confirmation output device indicating to a vending machine to complete a transaction.

41. The system according to claim 28, further comprising a transaction/identification records storage database.

42. The system according to claim 28, wherein said product comprises alcohol.

43. The system according to claim 28, wherein said product comprises cigarettes.

44. The system according to claim 28, wherein said product comprises firearms.

45. The system according to claim 28, wherein said product comprises a prescription medication.

46. The system according to claim 28, wherein said product comprises an airline seat.

47. The system according to claim 28, wherein said product comprises a casino admission.

48. The system according to claim 28, wherein said product comprises a mature-content performance admission.

49. The system according to claim 28, wherein said product comprises a pathogenic organism.

50. The system according to claim 28, wherein said product comprises a chemical.

51. The system according to claim 28, wherein biometric information receiver is located at a vendor.

52. The system according to claim 28, wherein said biometric information receiver is located at a home of said potential customer.

53. The system according to claim 28, wherein said biometric information receiver comprises a voice recognition device connected to a telephone line.

54. The system according to claim 28, wherein said telephone line comprises a product ordering line.

55. A system comprising:

means for receiving biometric identification information from a potential customer;

means for identifying a group membership of said potential customer; and

means for confirming to a vendor a right of said potential customer to purchase a product.

56. A computer readable medium containing program instructions for execution on a computer system, which when executed by the computer system, cause the computer system to perform the method recited in any one of claims 1 to 27.

| RESTRICTED PRODUCT | PROHIBITED GROUP | GROUNDS FOR PROHIBITION | UNIQUE DIFFICULTIES ENFORCING PROHIBITION |
|---|---|---|---|
| Alcohol | Underaged | -Protect Prohibited Group<br>-Prevent Operation of Automobiles after Alcohol Consumption by the Prohibited Group<br>-Reduce Liability of Society to (Ultimately) Provide for Welfare of Prohibited Group | -Widespread Indifference among Vendors and General Public<br>-Falsification of Identity Documents |
| Cigarettes | Underaged | -Protect Prohibited Group<br>-Protect Society from "Second-hand Smoke" Generated by Prohibited Group<br>-Reduce Liability of Society to (Ultimately) Provide for Welfare of Prohibited Group | -Widespread Indifference among Vendors and General Public<br>-Cigarette Vending Machines |
| Firearms | Underaged | -Protect Prohibited Group<br>-Protect Society from Unsafe Operation of Firearms by Prohibited Group | -Gun Show Sales<br>-Burden of Enforcement |
| Firearms | "Criminals" | -Protect Society from Unsafe Operation of Firearms by Prohibited Group | -Gun Show Sales<br>-Burden of Enforcement |
| Prescription Medication | Those Lacking A Physician's Presciption | -Protect Prohibited Group<br>-Protect Society from Unsafe Use/Abuse of Prescription Medication by Prohibited Group<br>-Prevent Distribution of Prescription Medication by Prohibited Group to Others<br>-Reduce Liability of Society to Provide for Welfare of Prohibited Group | |
| Seating in Airplanes | Underaged | -Ensure Safe Operation of Emergency Exits | -Widespread Indifference among Vendors and General Public<br>-Telephone/Internet Reservations |
| Casino Admission | Underaged | -Protect Prohibited Group<br>-Protect Portions of Society Liable for Financial Transactions of Prohibited Group<br>-Reduce Liability of Society to (Ultimately) Provide for Welfare of Prohibited Group | -Widespread Indifference among Vendors and General Public<br>-Falsification of Identity Documents |
| Admission to Mature-Content Performances | Underaged | -Protect Prohibited Group<br>-Reduce Liability of Society to Provide for Welfare of Prohibited Group | -Widespread Indifference among Vendors and General Public<br>-Falsification of Identity Documents |
| Pathogenic Organisms | Unlicensed Individuals | -Protect Prohibited Group<br>-Protect Society from Unsafe Use/Abuse of Pathogenic Organisms by Prohibited Group | -Burden of Enforcement |
| Chemicals | Unlicensed Individuals | -Protect Prohibited Group<br>-Protect Society from Unsafe Use/Abuse of Research Chemicals by Prohibited Group | -Burden of Enforcement |

FIG.1

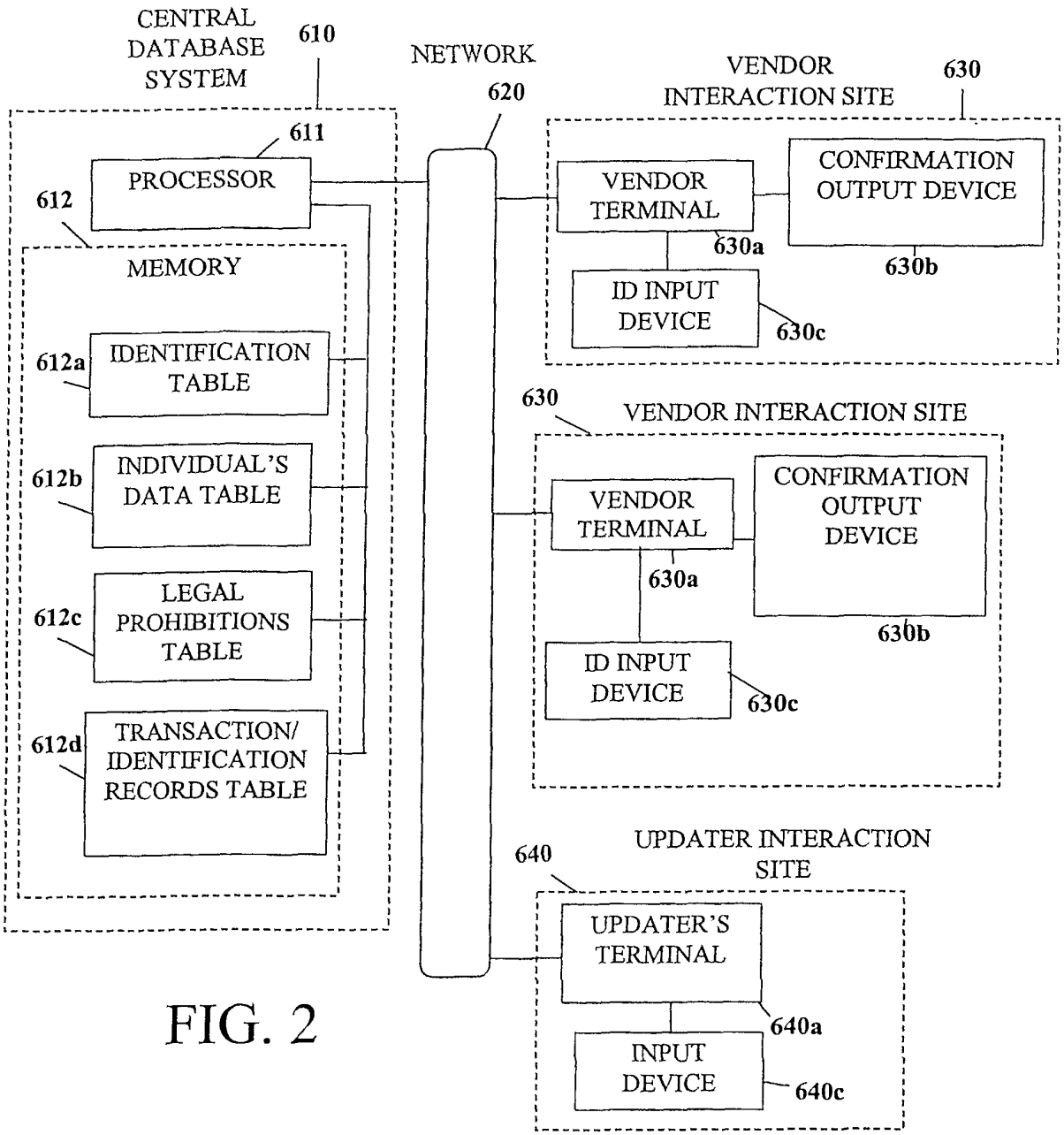

CENTRAL DATABASE SYSTEM
610
NETWORK
620
VENDOR INTERACTION SITE
630
611
PROCESSOR
612
MEMORY
612a
IDENTIFICATION TABLE
612b
INDIVIDUAL'S DATA TABLE
612c
LEGAL PROHIBITIONS TABLE
612d
TRANSACTION/ IDENTIFICATION RECORDS TABLE
VENDOR TERMINAL
630a
CONFIRMATION OUTPUT DEVICE
630b
ID INPUT DEVICE
630c
630
VENDOR INTERACTION SITE
VENDOR TERMINAL
630a
CONFIRMATION OUTPUT DEVICE
630b
ID INPUT DEVICE
630c
640
UPDATER INTERACTION SITE
UPDATER'S TERMINAL
640a
INPUT DEVICE
640c

FIG. 2

| DATA RECORD A | |
|---|---|
| START INDICATOR | 710a |
| RECORD ID # | 710b |
| POT. CONSUMER'S NAME | 710c |
| BIOMETRIC ID FACTOR 1 | 710d |
| BIOMETRIC ID FACTOR 2 | 710e |
| BIOMETRIC ID FACTOR N | 710f |
| END INDICATOR | 710g |

710

FIG. 3a

| DATA RECORD B | |
|---|---|
| START INDICATOR | 720a |
| RECORD ID # | 720b |
| POT. CONSUMER'S NAME | 720c |
| INDIVIDUAL INFO 1 | 720d |
| INDIVIDUAL INFO 2 | 720e |
| INDIVIDUAL INFO 3 | 720f |
| INDIVIDUAL INFO N | 720g |
| END INDICATOR | 720h |

720

FIG. 3b

| DATA RECORD C | |
|---|---|
| START INDICATOR | 730a |
| RECORD ID # | 730b |
| JURISDICTION NAME | 730c |
| RESTRICTION INFO 1 | 730d |
| RESTRICTION INFO 2 | 730e |
| RESTRICTION INFO 3 | 730f |
| RESTRICTION INFO 4 | 730g |
| RESTRICTION INFO N | 730h |
| END INDICATOR | 730i |

730

FIG. 4a

| DATA RECORD D | |
|---|---|
| START INDICATOR | 740a |
| RECORD ID # | 740b |
| CONSUMER'S NAME | 740c |
| JURISDICTION NAME | 740d |
| TRANSACTION INFO | 740e |
| BIOMETRIC ID FACTOR 1 | 740f |
| BIOMETRIC ID FACTOR 2 | 740g |
| BIOMETRIC ID FACTOR 3 | 740h |
| BIOMETRIC ID FACTOR N | 740i |
| END INDICATOR | 740j |

FIG. 4b

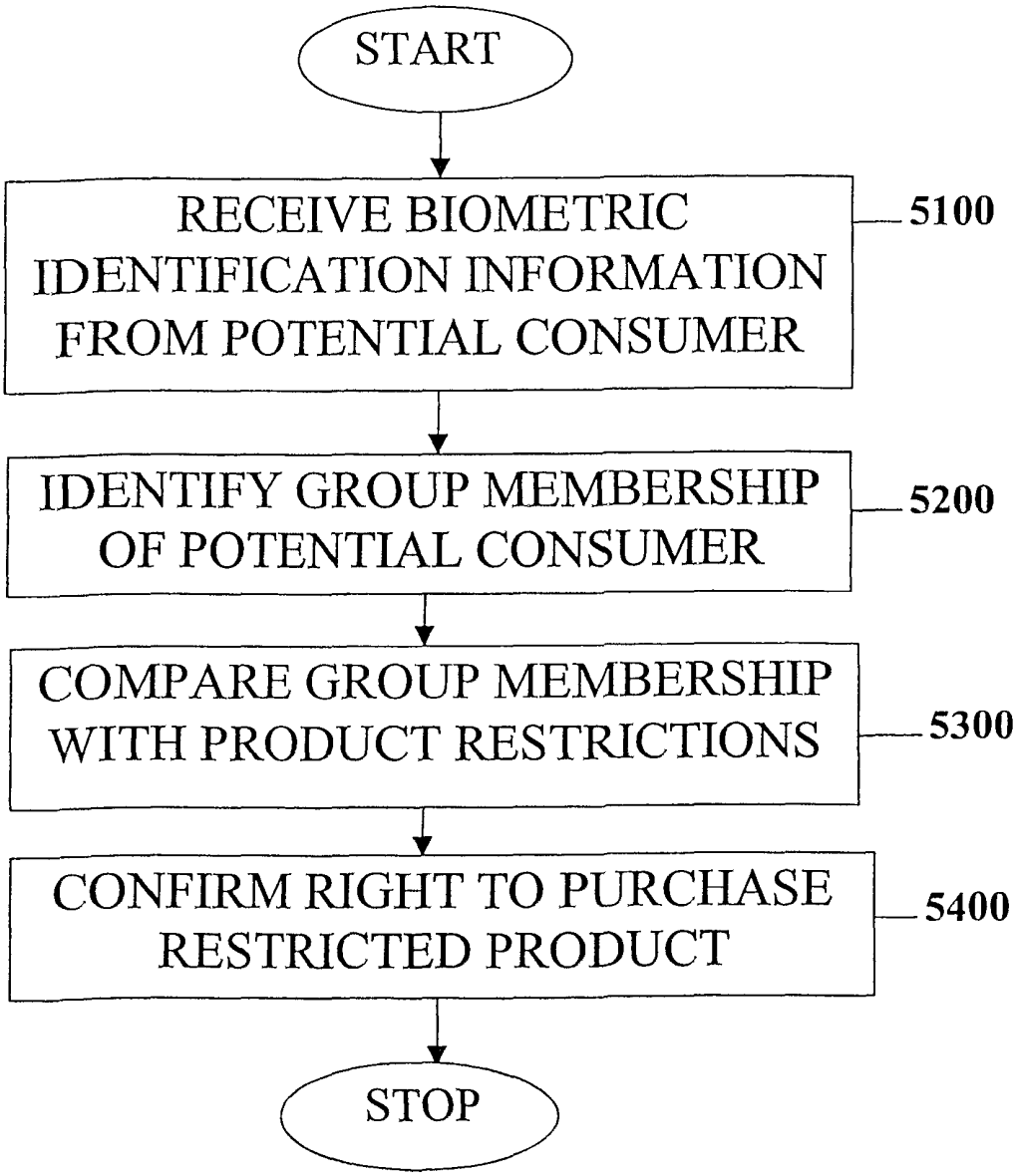

START
RECEIVE BIOMETRIC IDENTIFICATION INFORMATION FROM POTENTIAL CONSUMER
5100
IDENTIFY GROUP MEMBERSHIP OF POTENTIAL CONSUMER
5200
COMPARE GROUP MEMBERSHIP WITH PRODUCT RESTRICTIONS
5300
CONFIRM RIGHT TO PURCHASE RESTRICTED PRODUCT
5400
STOP

FIG. 5

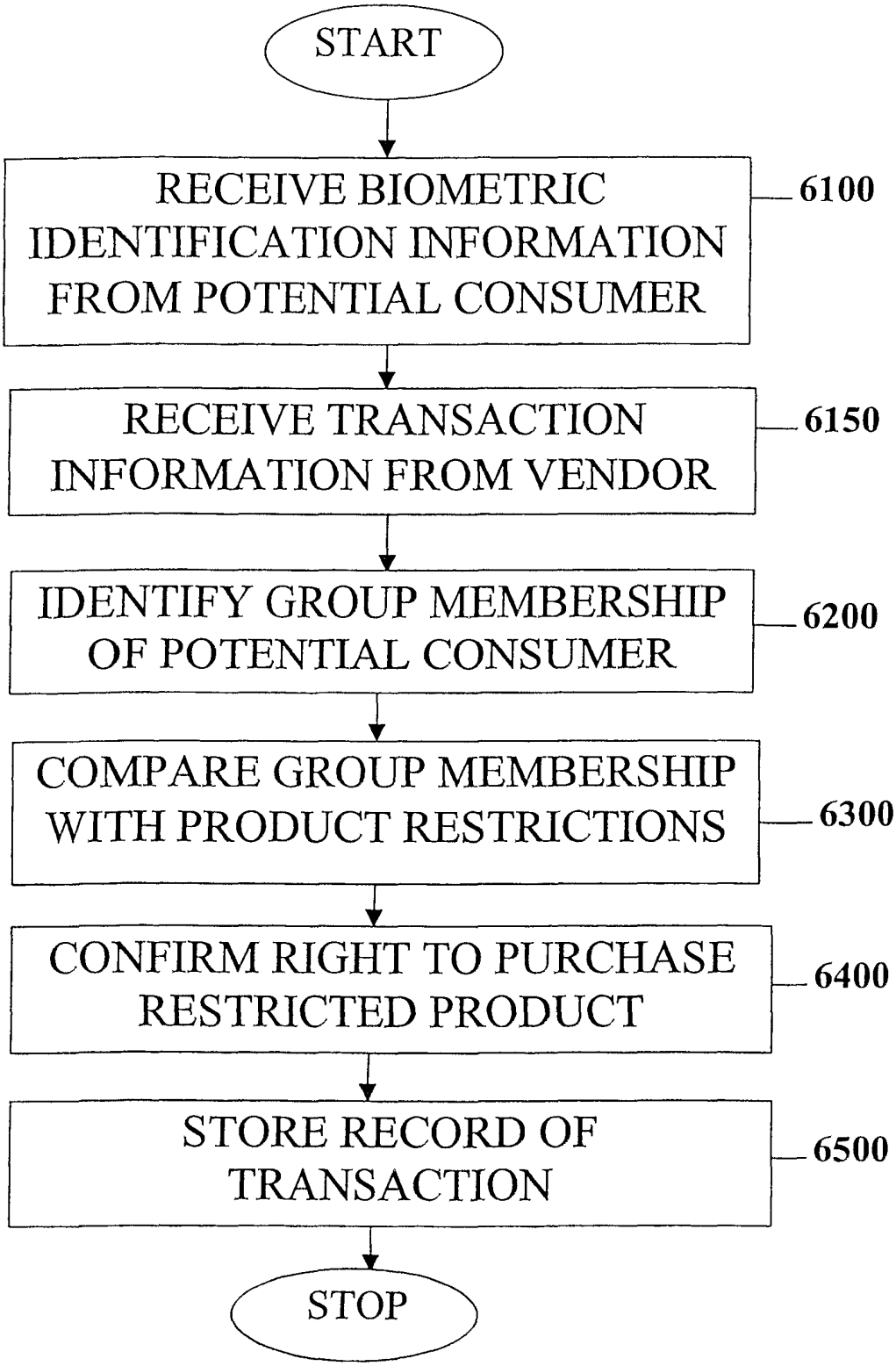

START
RECEIVE BIOMETRIC IDENTIFICATION INFORMATION FROM POTENTIAL CONSUMER
6100
RECEIVE TRANSACTION INFORMATION FROM VENDOR
6150
IDENTIFY GROUP MEMBERSHIP OF POTENTIAL CONSUMER
6200
COMPARE GROUP MEMBERSHIP WITH PRODUCT RESTRICTIONS
6300
CONFIRM RIGHT TO PURCHASE RESTRICTED PRODUCT
6400
STORE RECORD OF TRANSACTION
6500
STOP

FIG. 6

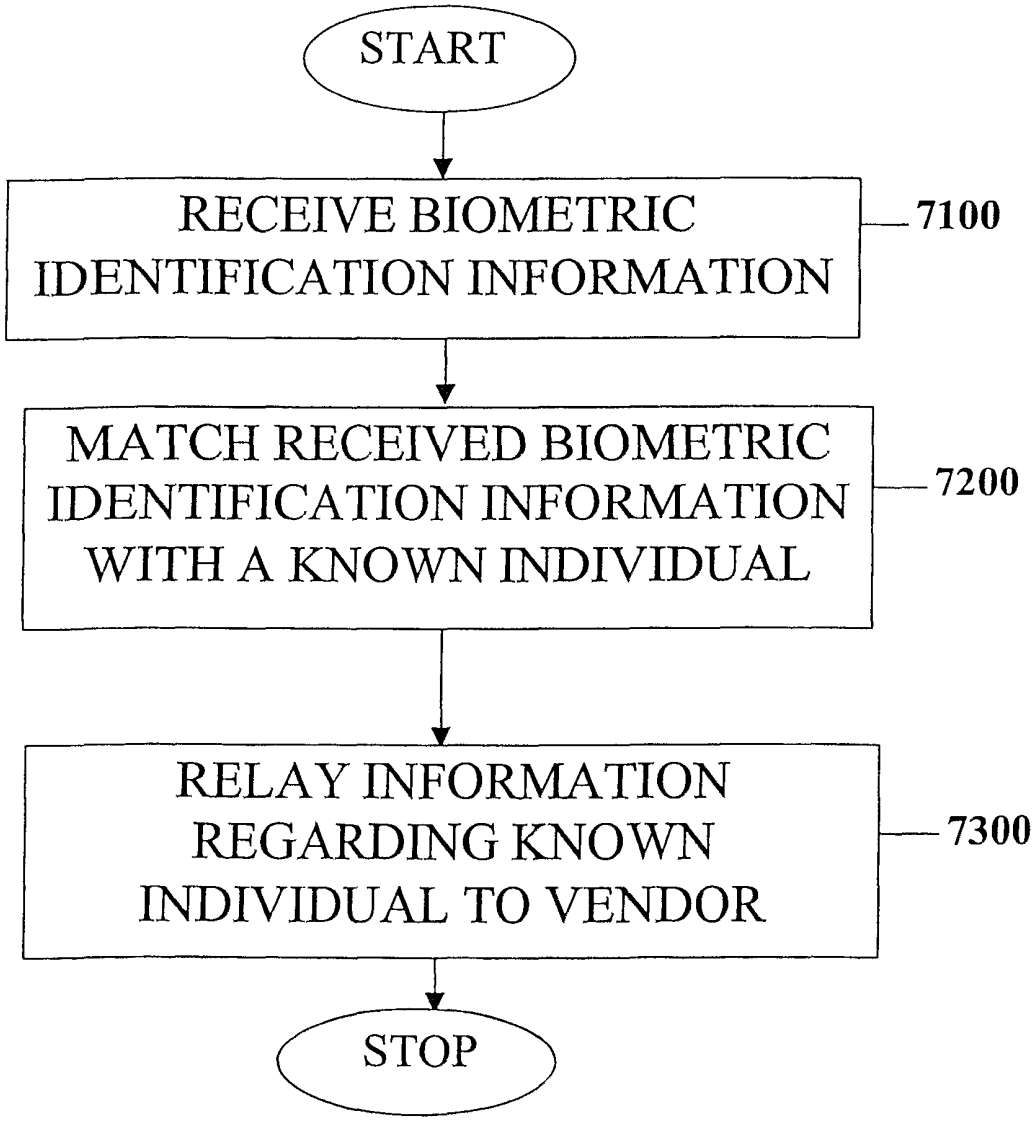

START
RECEIVE BIOMETRIC IDENTIFICATION INFORMATION
7100
MATCH RECEIVED BIOMETRIC IDENTIFICATION INFORMATION WITH A KNOWN INDIVIDUAL
7200
RELAY INFORMATION REGARDING KNOWN INDIVIDUAL TO VENDOR
7300
STOP

FIG. 7

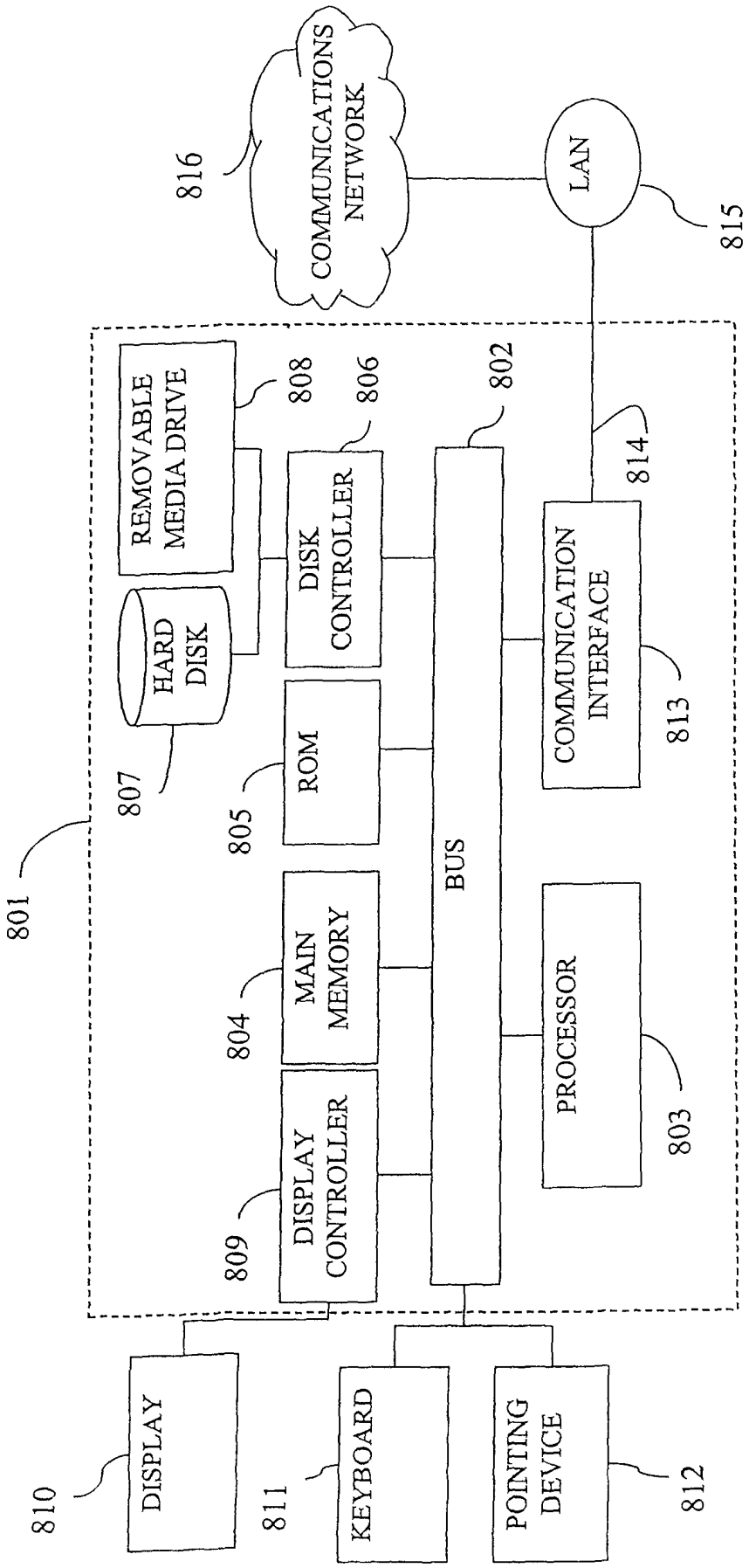

COMMUNICATIONS NETWORK
816
LAN
815
801
REMOVABLE MEDIA DRIVE
808
DISK CONTROLLER
806
802
HARD DISK
807
ROM
805
COMMUNICATION INTERFACE
814
813
MAIN MEMORY
804
BUS
PROCESSOR
803
DISPLAY CONTROLLER
809
DISPLAY
810
KEYBOARD
811
POINTING DEVICE
812

FIG. 8

# INTERNATIONAL SEARCH REPORT

Ir onal Application No
PCT/US 01/00677

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C9/00

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)
IPC 7 G07C G07F G06F A61J

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 96 21925 A (OMNICELL TECHNOLOGIES INC)<br>18 July 1996 (1996-07-18)<br>the whole document<br>--- | 1-56 |
| X | WO 00 60449 A (SCRIPTPRO LLC)<br>12 October 2000 (2000-10-12)<br>the whole document<br>---<br>-/-- | 1,5,<br>9-13,<br>15-19,<br>26-29,<br>33,34,<br>37,40,<br>41,45,<br>49-52,<br>54-56 |

[X] Further documents are listed in the continuation of box C

[X] Patent family members are listed in annex.

° Special categories of cited documents :

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

"E" earlier document 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 | Date of mailing of the international search report |
|---|---|
| 14 August 2001 | 24/08/2001 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax (+31-70) 340-3016 | Guivol, O |

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No |
|---|---|---|
| X | DE 197 47 353 A (LAUMER AXEL)<br>29 April 1999 (1999-04-29)<br><br>the whole document | 1,5,<br>9-13,15,<br>17-21,<br>24-29,<br>41,45,<br>49-56 |
| Y | US 1 855 200 A (HANS REICHERT)<br>26 April 1932 (1932-04-26)<br><br>the whole document | 1-3,<br>11-13,<br>15-19,<br>28,29,<br>37-41,55 |
| Y | US 5 722 526 A (SHARRARD ROBERT C)<br>3 March 1998 (1998-03-03)<br><br>the whole document | 1-3,<br>11-13,<br>15-19,<br>28,29,<br>37-41,55 |
| E | DE 199 44 140 A (SCHULZE LOEWEN AUTOMATEN)<br>29 March 2001 (2001-03-29)<br><br>column 2, line 68 -column 3, line 55 | 1,6,<br>11-13,<br>17-20,<br>28,29,<br>33,40,<br>47,51,<br>55,56 |
| X | US 5 459 957 A (WINER GUY T)<br>24 October 1995 (1995-10-24)<br><br>the whole document | 1,4,15,<br>21,28,<br>29,33,<br>37,44,<br>53,55 |
| X | US 5 937 557 A (BOWKER J KENT ET AL)<br>17 August 1999 (1999-08-17)<br><br>abstract<br>column 27, line 34 - line 40 | 1,4,10,<br>17,28,<br>29,33,<br>44,50,55 |

-/--

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No |
|---|---|---|
| X | WO 97 24702 A (GILMORE JANICE FANT)<br>10 July 1997 (1997-07-10)<br><br>page 12, line 12 -page 13, line 2<br>page 18, line 3 - line 14; claims 5,6;<br>figures 1,2,6,10 | 1,5,<br>9-15,<br>17-21,<br>23,24,<br>28,29,<br>31-35,<br>37-41,<br>45,49-56 |
| A | EP 0 991 027 A (NCR INT INC)<br>5 April 2000 (2000-04-05)<br>the whole document | 1-56 |
| A | US 4 915 205 A (REID JOHN N ET AL)<br>10 April 1990 (1990-04-10)<br>column 2, line 29 - line 35<br>column 6, line 42 - line 46 | 7 |
| A | US 5 867 802 A (BORZA STEPHEN J)<br>2 February 1999 (1999-02-02)<br><br>abstract; claims; figures | 1,15-18,<br>26,28,<br>33,37,<br>55,56 |
| A | US 5 224 173 A (KUHNS ROGER J ET AL)<br>29 June 1993 (1993-06-29)<br>the whole document | 1-56 |
| A | WO 96 18169 A (KRETZSCHMAR LOREN ;DAVIS VICTORIA (US)) 13 June 1996 (1996-06-13)<br><br>the whole document | 1,11-13,<br>17-21,<br>26-29,<br>31-34,<br>40,41,<br>51,52,<br>54,55 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ional Application No
PCT/US 01/00677

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9621925 A | 18-07-1996 | AU 4691096 A | 31-07-1996 |
| WO 0060449 A | 12-10-2000 | AU 3928800 A | 23-10-2000 |
| | | AU 4049200 A | 23-10-2000 |
| | | WO 0059730 A | 12-10-2000 |
| | | US 6206590 B | 27-03-2001 |
| DE 19747353 A | 29-04-1999 | NONE | |
| US 1855200 A | 26-04-1932 | NONE | |
| US 5722526 A | 03-03-1998 | NONE | |
| DE 19944140 A | 29-03-2001 | NONE | |
| US 5459957 A | 24-10-1995 | NONE | |
| US 5937557 A | 17-08-1999 | US 5812252 A | 22-09-1998 |
| | | AU 4973696 A | 27-08-1996 |
| | | CA 2211910 A | 15-08-1996 |
| | | EP 0811203 A | 10-12-1997 |
| | | WO 9624283 A | 15-08-1996 |
| WO 9724702 A | 10-07-1997 | AU 1356597 A | 28-07-1997 |
| | | CA 2241082 A | 10-07-1997 |
| | | GB 2324080 A,B | 14-10-1998 |
| | | US 6138865 A | 31-10-2000 |
| EP 0991027 A | 05-04-2000 | JP 2000187777 A | 04-07-2000 |
| US 4915205 A | 10-04-1990 | AU 588909 B | 28-09-1989 |
| | | AU 6224886 A | 05-03-1987 |
| | | DE 3688189 A | 06-05-1993 |
| | | DE 3688189 D | 06-05-1993 |
| | | EP 0231319 A | 12-08-1987 |
| | | WO 8700948 A | 12-02-1987 |
| | | JP 63501176 T | 28-04-1988 |
| US 5867802 A | 02-02-1999 | CA 2156236 A | 17-02-1997 |
| US 5224173 A | 29-06-1993 | NONE | |
| WO 9618169 A | 13-06-1996 | AU 4894796 A | 26-06-1996 |